

(12) 特許協力条約に基づいて公開された国際出願

10/517258

(19) 世界知的所有権機関  
国際事務局



(43) 国際公開日  
2003年12月24日 (24.12.2003)

PCT

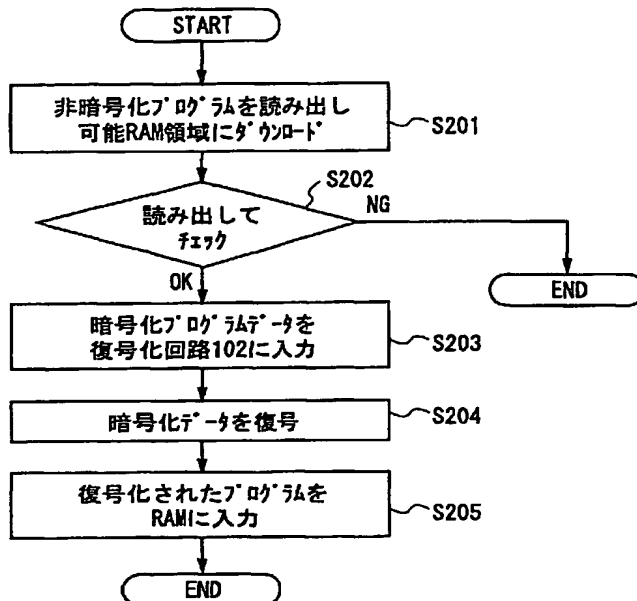
(10) 国際公開番号  
WO 03/107193 A1

- (51) 国際特許分類: G06F 12/14, 1/00 (72) 発明者; および  
(21) 国際出願番号: PCT/JP03/07541 (75) 発明者/出願人 (米国についてのみ): 中井 勝  
(22) 国際出願日: 2003年6月13日 (13.06.2003) 博 (NAKAI, Katsuhiko) [JP/JP]; 〒669-1321 兵庫県  
(25) 国際出願の言語: 日本語 三田市 けやき台 4-43-4 Hyogo (JP). 難波 剛  
(26) 国際公開の言語: 日本語 (NANBA, Tsuyoshi) [JP/JP]; 〒573-1118 大阪府 枚  
(30) 優先権データ: 特願2002-174883 2002年6月14日 (14.06.2002) JP 方市 楠葉並木 2-24-16 Osaka (JP). 平野 雄久  
(71) 出願人 (米国を除く全ての指定国について): 松下電 (HIRANO, Takehisa) [JP/JP]; 〒562-0022 大阪府 箕  
器産業株式会社 (MATSUSHITA ELECTRIC INDUS- 面市 粟生間谷東 6-7-9 Osaka (JP). 手塚 智明  
TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 (TEZUKA, Tomoaki) [JP/JP]; 〒533-0021 大阪府 大阪  
大字門真 1006番地 Osaka (JP). 市 東淀川区下新庄 2-12-21-301 Osaka (JP).  
(74) 代理人: 早瀬 憲一 (HAYASE, Kenichi); 〒532-0003 大  
阪府 大阪市 淀川区宮原 3丁目4番30号 ニッセイ  
新大阪ビル 13階 早瀬特許事務所 Osaka (JP).  
(81) 指定国 (国内): CN, JP, US.

[続葉有]

(54) Title: SEMICONDUCTOR INTEGRATED CIRCUIT DEVICE, DATA STORAGE VERIFICATION DEVICE, AND DATA STORAGE VERIFICATION METHOD

(54) 発明の名称: 半導体集積回路装置、データ記憶検証装置およびデータ記憶検証方法



- S201...READ OUT NON-ENCRYPTED PROGRAM AND DOWNLOAD IT INTO A POSSIBLE RAM AREA  
S202...READ OUT AND CHECK  
S203...INPUT ENCRYPTED PROGRAM DATA IN DECRYPTING CIRCUIT 102  
S204...DECRYPT THE ENCODED DATA  
S205...INPUT THE DECRYPTED PROGRAM INTO RAM

(57) Abstract: A semiconductor integrated circuit device (100) for downloading a program of a processing unit such as a DSP and a CPU from outside. When a rewrite program which is secret information not to be leaked to a third person is downloaded in a semiconductor integrated circuit (109), it is possible to check whether the rewrite program has been correctly downloaded while maintaining the secrecy. The semiconductor integrated circuit device includes a circuit for verifying the content of the downloaded rewrite program and/or a program for verifying the content of the downloaded rewrite program.

(57) 要約: DSPやCPUなどの演算処理ユニットのプログラムを外部からダウンロードする半導体集積回路装置(100)において、半導体集積回路(109)内にダウンロードした、第三者に漏洩したくない機密情報である書き換えプログラムを、その機密を保持しながら該書き換えプログラムが正しくダウンロードできたか否かの確認を可能とする半導体集積回路装置を提供する。ダウンロードした書き換えプログラムの内容を検証する回路、及び/またはダウンロードした書き換えプログラムの内容を検証するプログラムを備える。

WO 03/107193 A1



(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

## 明 細 書

## 半導体集積回路装置、データ記憶検証装置およびデータ記憶検証方法

## 5 技術分野

本発明は半導体集積回路装置、データ記憶検証装置およびデータ記憶検証方法に関するものであり、特に、内容が第三者へ漏洩したくない機密情報であるプログラムの保護、すなわちその機密性を維持しながら、ダウンロードが確実に実行できたか否かを容易に確認できるようにしたものに関する。

10

## 背景技術

DSP (Digital Signal Processor) やCPUなどの演算処理ユニットを含む半導体集積回路において、演算処理ユニットのプログラムは、コスト面やプログラムの機密性を保つという点においてはROMとしてプログラムを格納することが有利となる。しかしながら、ROMなどの書き換え不可能な手段でプログラムを保持した場合、仕様変更やプログラム自身の不具合に柔軟な対応が取りにくい。このような回路の開発における容易さなどの点から、プログラムを半導体集積回路内部に格納する手段を、RAMなどの書き換え可能な手段として所有することがある。このような構成を持つ回路においては、DSPやCPUのような信号処理・機器の制御を担う演算処理ユニットなどに必要なプログラムを事前に書き換え可能なRAMなどの指定領域にダウンロードする必要があった。なお、本明細書において、ダウンロードとは、データやプログラムを、半導体集積回路の内部にロードする、ことを意味するものとする。

しかし、DSPやCPUなどの演算処理ユニットのプログラムを外部からRAMにダウンロードする半導体集積回路においては、プログラムを半導体集積回路内部にROMで持っている場合よりもプログラムの内容が第三者に漏洩する危険が高いという欠点を有していた。

例えば、半導体集積回路外部に保持するプログラムが、著作権保護を目的として策定されたウォーターマーク（電子透かし）を検出するためのプログラムのよ

うな場合、プログラムの内容が悪意を持った第三者に漏洩したことによって、著作権保護のための仕組みを無効化される恐れがあるため、プログラム自身を保護する必要がある。

- 5      この場合、半導体集積回路内にダウンロードするプログラムを予め暗号化させて、該半導体集積回路内で復号化させることにより、プログラム自身を保護することが考えられる。

しかしながら、この予め暗号化したデータ、及び非暗号化データも含めて半導体集積回路内の書き換え可能な領域にダウンロードしたプログラムデータが正しく格納できたか否かを、機密性を保持しながら確認することは困難である。

- 10      本発明はこのような問題を解決するためになされたものであり、機密性を要するプログラムデータを外部に漏らすことなく、正しくダウンロードできたか否かを確認できる半導体集積回路装置、データ記憶検証装置およびデータ記憶検証方法を提供することを目的とする。

## 15      発明の開示

- 上記問題を解決するために、本発明の請求の範囲第1項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第2の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、上記第2の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第1の格納手段からの上記書き換えプログラムを、上記第2の格納手段の外部読出し不可能領域に格納するようにしたものである。

これにより、例えばダミーデータなどを、上記第2の格納手段の読み出し可能

な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、半導体集積回路内に正しく上記書き換えプログラムが格納されたかどうかを、該書き換えプログラムの機密性を保持しながら確認することができる。

- また、本発明の請求の範囲第2項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第2の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えたものである。

- これにより、上記第2の格納手段に格納された特定部分のみを読み出して、該特定部分を検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第3項に記載の半導体集積回路装置は、請求の範囲第2項に記載の半導体集積回路装置において、上記制御回路は、上記第2の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとしたものである。

- これにより、上記第2の格納手段の特定のアドレスのみを読み出して、該特定のアドレスのデータを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

- また、本発明の請求の範囲第4項に記載の半導体集積回路装置は、請求の範囲第2項に記載の半導体集積回路装置において、上記制御回路は、上記第2の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとしたものである。

これにより、上記第2の格納手段の特定のビットのみを読み出して、該特定のビットのみを検証することにより、上記書き換えプログラムが半導体集積回路内

に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

- また、本発明の請求の範囲第5項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第2の格納手段に格納した上記書き換えプログラムの一部を実行するものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

- また、本発明の請求の範囲第6項に記載の半導体集積回路装置は、請求の範囲第5項に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである。

- これにより、例えば、上記第2の格納手段に格納された上記書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる。

- また、本発明の請求の範囲第7項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第1の格納手段から上記第2の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えたものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第 8 項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第 2 の格納手段を半導体集積回路内に有し、該第 2 の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第 1 の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、上記第 2 の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、上記第 2 の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行うものである。

これにより、接続切り換え手段にて演算処理ユニットのプログラム入力またはデータ入力を切り替えて、上記書き換えプログラムのデータを取り込んで、例えば該書き換えプログラムデータのチェックサムなどをとって、予め決めておいた値と比較することが可能になるので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第 9 項に記載の半導体集積回路装置は、請求の範囲第 8 項に記載の半導体集積回路装置において、上記第 2 の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとしたものである。

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半

導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

- 5     また、本発明の請求の範囲第10項に記載の半導体集積回路装置は、請求の範囲第9項に記載の半導体集積回路装置において、上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用するものである。

- 10    これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

- 15    また、本発明の請求の範囲第11項に記載の半導体集積回路装置は、請求の範囲第8項に記載の半導体集積回路装置において、上記第2の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次2分割した構成とし、該2分割した各々の領域に同じプログラムデータを格納するものであり、上記チェックプログラムは、上記2分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、前回の判定結果が正しいと  
20    判定されたときに、前回2分割した領域の一方の領域を、プログラムが格納されていない領域としてさらに2分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、上記第2の格納手段に格納すべきプログラムすべてを順次格納するものである。

- 25    これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

また、本発明の請求の範囲第12項に記載の半導体集積回路装置は、請求の範



図第 1 1 項に記載の半導体集積回路装置において、上記第 2 の格納手段は、該第 2 の格納手段の上記書き換えプログラムが格納されていない領域を順次 2 分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとしたものである。

- 5      これにより、例えば、第 2 の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第 2 の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第 2 の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

- 10      また、本発明の請求の範囲第 1 3 項に記載の半導体集積回路装置は、請求の範囲第 1 2 項に記載の半導体集積回路装置において、上記一意に得られるデータが、該プログラムデータの反転データであるものとしたものである。

- 15      これにより、例えば、第 2 の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第 2 の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第 2 の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

- 20      また、本発明の請求の範囲第 1 4 項に記載の半導体集積回路装置は、請求の範囲第 8 項ないし第 1 3 項のいずれかに記載の半導体集積回路装置において、上記チェックプログラムを予め格納した ROM (Read Only Memory) を備え、上記 ROM により上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行うものである。

- 25      これにより、上記チェックプログラムの転送誤り等により、チェックプログラムが機能しなくなるのを防ぎ、上記第 2 の格納手段に上記書き換えプログラムが正しく格納できたか否かを確認するチェックプログラムを安定的に提供することができる効果がある。

また、本発明の請求の範囲第 1 5 項に記載の半導体集積回路装置は、請求の範囲第 1 項ないし第 1 4 項のいずれかに記載の半導体集積回路装置において、上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を

備え、上記第1の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第2の格納手段に復号化した上記書き換えプログラムを格納するものである。

5 これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第16項に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該  
10 第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第1の格納手段から  
15 グラムを上記第2の格納手段に転送する復号化手段と、上記第2の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、上記暗号化手段で暗号化された書き換えプログラムと上記第1の格納手段に保持している暗号化された書き換えプログラムとを比較するものである。

20 これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第17項に記載の半導体集積回路装置は、請求の範囲第11項ないし第13項、及び第16項のいずれかに記載の半導体集積回路装置において、上記第2の格納手段にデータが正しく格納されていない場合、不良  
25 箇所を検出し、上記第1の格納手段に保持した書き換えプログラムを修正可能としたものである。

これにより、第2の格納手段において正しく格納できなかった箇所を使用しないように書き換えプログラムを修正して書き込むので、メモリを有効に活用することができる。

また、本発明の請求の範囲第 18 項に記載の半導体集積回路装置は、請求の範囲第 1 項ないし第 17 項のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたものである。

- 5      これにより、書き換えプログラムを半導体集積回路装置外部に有する場合においても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる。

- 10      また、本発明の請求の範囲第 19 項に記載のデータ記憶検証装置は、任意のデータを外部からアクセス可能な領域に記憶させる手段と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる手段とを備えた、ことを特徴とするものである。

- 15      これにより、例えばダミーデータなどを、上記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく上記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

- 20      また、本発明の請求の範囲第 20 項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域に記憶させる手段と、前記機密データの特定部分を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データの特定部分のみを読み出して、該特定部分を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

- 25      また、本発明の請求の範囲第 21 項に記載のデータ記憶検証装置は、プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる手段と、前記記憶されたプログラムを実行させ、結果を外部に出力する手段とを備えた、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データに含まれ

ているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

- 5 また、本発明の請求の範囲第22項に記載のデータ記憶検証装置は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第1の手段と、前記検査プログラムを実行させ、結果を外部に出力する第2の手段と、前記第2の手段の終了後、前記機密プログラムを実行させる第3の手段とを備えた、ことを特徴とするものである。

- 10 これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

- 15 また、本発明の請求の範囲第23項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な領域に記憶させる手段と、前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、前記演算の結果を外部に出力する手段とを備えた、ことを特徴とするものである。

- 20 これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

- 25 また、本発明の請求の範囲第24項に記載のデータ記憶検証装置は、機密データを外部からアクセス不可能な第1の領域に記憶させる第4の手段と、機密データの一部であり、前記第1の領域に記憶されている検査プログラムを第2の領域に記憶させる第5の手段と、前記第2の領域に記憶されている検査プログラムを実行して、前記第1の領域の機密データの正当性を検査する第6の手段とを備えた、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第1の領域に格納するとともに、その機密データの一部である検査プログラムを第2の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第1の

領域の機密データの正当性を検証することにより、上記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

- 5      また、本発明の請求の範囲第 2 5 項に記載のデータ記憶検証装置は、請求項 2 4 記載のデータ記憶検証装置において、前記第 6 の手段の終了後に前記第 1 の領域の命令に制御を移す第 7 の手段をさらに備えた、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認した後に、本来の機密データに含まれる命令の実行に移ることができる。

- 10      また、本発明の請求の範囲第 2 6 項に記載のデータ記憶検証装置は、請求項 2 4 記載のデータ記憶検証装置において、前記第 5 の手段は、前記第 1 の領域に記憶されている機密データ内に存在する命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

- 15      これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データ内に存在する命令により行うことができる。

- 20      また、本発明の請求の範囲第 2 7 項に記載のデータ記憶検証装置は、請求項 2 4 記載のデータ記憶検証装置において、前記第 5 の手段は、第 3 の領域に前記第 4 の手段による記憶の実行以前に記憶された命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

- 25      また、本発明の請求の範囲第 2 8 項に記載のデータ記憶検証装置は、機密データを復号する手段と、前記復号されたデータを外部からアクセス不可能な領域に記憶させる手段と、前記記憶されたデータを暗号化する手段と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する手段とを備えた、ことを特徴とするものである。

これにより、いったん復号して外部からアクセス不可能な領域に格納した機密

データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第 29 項に記載のデータ記憶検証装置は、機密プログラムを外部からアクセス不可能な領域に記憶させる手段と、前記記憶されたプログラムを読み出す手段と、前記読み出されたプログラムを命令単位で正当性を判定する手段と、正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域において空いている領域に記憶させる手段と、前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスにジャンプする命令を記憶させる手段と、正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる手段とを備えた、ことを特徴とするものである。

これにより、機密プログラムを外部からアクセス不可能な領域に格納し、その格納したプログラムを読み出し命令単位で正当性を判定し、正当でないと判定された命令に対しては外部からアクセス不可能な領域の空き領域に格納した正当な命令にジャンプすることにより、機密プログラムを格納する際にその一部に正しく格納できていない命令が含まれていても、空き領域に格納した正しい命令に置換してこれを実行することができる。

また、本発明の請求の範囲第 30 項に記載のデータ記憶検証方法は、任意のデータを外部からアクセス可能な領域に記憶させる工程と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる工程とを含む、ことを特徴とするものである。

これにより、例えばダミーデータなどを、前記外部からアクセス可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、外部からアクセス不可能な領域に正しく前記機密データが格納されたかどうかを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第 31 項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域に記憶させる工程と、前記機密データの特定

部分を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、外部からアクセス不可能な領域に格納された機密データの特定部分のみを読み出して、該特定部分を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第32項に記載のデータ記憶検証方法は、プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる工程と、前記記憶されたプログラムを実行させ、結果を外部に出力する工程とを含む、ことを特徴とするものである。

10 これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第33項に記載のデータ記憶検証方法は、検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第1の工程と、前記検査プログラムを実行させ、結果を外部に出力する第2の工程と、前記第2の工程の終了後、前記機密プログラムを実行させる第3の工程とを含む、ことを特徴とするものである。

20 これにより、外部からアクセス不可能な領域に格納された機密データに含まれているプログラムを実行し、その実行結果を外部に出力して、該実行結果を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながらより確実に確認することができる。

また、本発明の請求の範囲第34項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な領域に記憶させる工程と、前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、前記演算の結果を外部に出力する工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な領域に格納するとともに、その機密データを用いて所定の演算を行い、その演算結果を外部に出力して、該演算結果を検証することにより、前記機密データが正しくダウンロードできたか

否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第 3 5 項に記載のデータ記憶検証方法は、機密データを外部からアクセス不可能な第 1 の領域に記憶させる第 4 の工程と、機密データの一部であり、前記第 1 の領域に記憶されている検査プログラムを第 2 の領域  
5 に記憶させる第 5 の工程と、前記第 2 の領域に記憶されている検査プログラムを実行して、前記第 1 の領域の機密データの正当性を検査する第 6 の工程とを含む、ことを特徴とするものである。

これにより、機密データを外部からアクセス不可能な第 1 の領域に格納するとともに、その機密データの一部である検査プログラムを第 2 の領域に格納し、この検査プログラムを用いて検査を行い、その検査結果を外部に出力して、第 1 の  
10 領域の機密データの正当性を検証することにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

また、本発明の請求の範囲第 3 6 項に記載のデータ記憶検証方法は、請求項 3  
15 5 記載のデータ記憶検証方法において、前記第 6 の工程の終了後に前記第 1 の領域の命令に制御を移す第 7 の工程をさらに含む、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認した後に、本来の機密データに含まれる命令の実行に移ることができる。

20 また、本発明の請求の範囲第 3 7 項に記載のデータ記憶検証方法は、請求項 3 5 記載のデータ記憶検証方法において、前記第 5 の工程は、前記第 1 の領域に記憶されている機密データ内に存在する命令により前記検査プログラムの記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データ  
25 の機密性を保持しながら確認するための検査プログラムの格納を、機密データ内に存在する命令により行うことができる。

また、本発明の請求の範囲第 3 8 項に記載のデータ記憶検証方法は、請求項 3 5 記載のデータ記憶検証方法において、前記第 5 の工程は、前記第 3 の領域に前記第 4 の工程による記憶の実行以前に記憶された命令により前記検査プログラム



の記憶を実行する、ことを特徴とするものである。

これにより、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認するための検査プログラムの格納を、機密データを格納するより前に格納した命令により行うことができる。

- 5      また、本発明の請求の範囲第 39 項に記載のデータ記憶検証方法は、機密データを復号する工程と、前記復号されたデータを外部からアクセス不可能な領域に記憶させる工程と、前記記憶されたデータを暗号化する工程と、前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータが正しく記憶されたか否かを判定する工程とを含む、ことを特徴とするものである。

- 10      これにより、いったん復号して外部からアクセス不可能な領域に格納した機密データを暗号化して、予め暗号化されている元の機密データと比較することで、前記機密データが正しくダウンロードできたか否かを、該機密データの機密性を保持しながら確認することができる。

- 15      また、本発明の請求の範囲第 40 項に記載のデータ記憶検証方法は、機密プログラムを外部からアクセス不可能な領域に記憶させる工程と、前記記憶されたプログラムを読み出す工程と、前記読み出されたプログラムを命令単位で正当性を判定する工程と、正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可能な領域において空いている領域に記憶させる工程と、前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次のアドレスに  
20      ジャンプする命令を記憶させる工程と、正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャンプする命令を記憶させる工程とを含む、ことを特徴とするものである。

- 25      これにより、機密プログラムを外部からアクセス不可能な領域に格納し、その格納したプログラムを読み出し命令単位で正当性を判定し、正当でないと判定された命令に対しては外部からアクセス不可能な領域の空き領域に格納した正当な命令にジャンプすることにより、機密プログラムを格納する際にその一部に正しく格納できていない命令が含まれていても、空き領域に格納した正しい命令に置換してこれを実行することができる。

## 図面の簡単な説明

- 第 1 図は、本発明の実施の形態 1 における半導体集積回路装置を示す図
- 第 2 図は、本発明の実施の形態 1 における半導体集積回路装置の動作を示すフローチャート
- 5 第 3 図は、本発明の実施の形態 2 における半導体集積回路装置を示す図
- 第 4 図は、本発明の実施の形態 2 における半導体集積回路装置の動作を示すフローチャート
- 第 5 図は、本発明の実施の形態 3 における半導体集積回路装置を示す図
- 第 6 図は、本発明の実施の形態 3 における半導体集積回路装置を示す図
- 10 第 7 図は、本発明の実施の形態 3 における半導体集積回路の実行プログラムの一例を示す図
- 第 8 図は、本発明の実施の形態 4 における半導体集積回路装置を示す図
- 第 9 図は、本発明の実施の形態 5 における半導体集積回路装置を示すブロック構成図
- 15 第 10 図は、本発明の実施の形態 5 における半導体集積回路装置の RAM（第 2 の格納手段）の構成の一例を示す構成図
- 第 11 図は、本発明の実施の形態 6 における半導体集積回路装置を示すブロック構成図
- 第 12 図は、本発明の実施の形態 6 における半導体集積回路装置の RAM（第 2 の格納手段）1106 の構成の一例を示す図
- 20 第 13 図は、本発明の実施の形態 6 におけるメモリ 1102 内のデータ配置を示す概念図
- 第 14 図は、本発明の実施の形態 7 における半導体集積回路装置を示すブロック構成図
- 25 第 15 図は、本発明の実施の形態 8 における半導体集積回路装置を示すブロック構成図
- 第 16 図は、本発明の実施の形態 8 における半導体集積回路装置の動作を示すフローチャート
- 第 17 図は、本発明の実施の形態 8 における半導体集積回路装置のプログラム

の修正を行う一例を示した図

発明を実施するための最良の形態

以下、本発明の実施の形態について、図を用いて説明する。

5 (実施の形態 1)

第 1 図は、本発明の実施の形態 1 に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、100 は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、例えば 105 は制御用マイコン、101 はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第 1 の格納手段）である。半導体集積回路 109 は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）102 と、書き換え可能な RAM（第 2 の格納手段）108 と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ 107 の処理を行う演算処理回路（演算処理ユニット）106 とから構成される。なお、書き換えプログラムは例えばこれを変更することで演算処理回路 106 に異なる機能を実現させるものである。

また、本発明の実施の形態 1 に係る半導体集積回路装置において、書き換え可能な RAM 108 は、半導体集積回路 109 の外部から読み出し可能な外部読み出し可能領域 103 と、半導体集積回路 109 の外部から読み出し不可能な外部読み出し不可能領域 104 とから構成される。この外部読み出し不可能領域 104 は、例えば、外部からのアドレスバスは外部読み出し可能領域 103 と同様外部読み出し不可能領域 104 に接続するが、外部にデータを読み出す場合はデータバスは外部読み出し不可能領域 104 には接続しないスイッチを設けること等で実現できる。

25 以上のように構成された半導体集積回路装置 100 について、第 2 図のフローチャートを用いてその動作を説明する。

制御用マイコン 105 の制御にしたがい、暗号化されていないデータを書き換え可能な RAM 108 の外部読み出し可能領域 103 に入力する（ステップ S 201）。次に、外部読み出し可能領域 103 に入力したデータが正しいかを半導体集積回路 109 外部に読み出して制御用マイコン 105 等でチェックする（ステップ

S 2 0 2)。ステップS 2 0 2でチェックした結果が正しい場合は、制御用マイコン1 0 5の制御にしたがいメモリ1 0 1の暗号化された書き換えプログラムを復号化回路1 0 2に入力し（ステップS 2 0 3）、復号化回路1 0 2は、暗号化された書き換えプログラムを復号する（ステップS 2 0 4）。次に、ステップS 2 0 4  
5 で復号化された書き換えプログラムを書き換え可能なRAM 1 0 8の外部読出し不可能領域1 0 4に入力する（ステップS 2 0 5）。以上の処理により、第三者に漏洩したくない書き換えプログラムの機密性を保ちながら、該書き換えプログラムが正しく格納されているか否かをチェックすることができる。

これは、上述のように暗号化されていないデータを外部から書き込み正しく読み出せたことは、これらを実行する回路に故障が生じていないと考えられるので、  
10 書き換えプログラムを外部読出し不可能領域1 0 4に格納する際にもこれを支障なく行えていると考えられるからである。

なお、書き換え可能なRAM 1 0 9の外部読出し可能領域1 0 3に格納するデータは、半導体集積回路装置の内部、及び外部のどちらに用意してもよく、  
15 チェック用のデータであればよい。

以上のような、本発明の実施の形態1に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムを書き換え可能なRAM 1 0 8に入力する場合に、該RAM 1 0 8に設けた外部読出し可能領域1 0 3、及び外部読出し不可能領域1 0 4のうち、外部読み出し可能領域1 0 3にチェック用のデータを格納し、該データのチェックの結果が正しいと判定された後、外部読  
20 出し不可能領域1 0 4に該機密情報のプログラムを格納することにより、第三者に漏洩したくない機密情報である書き換えプログラムを格納したRAM 1 0 8の製造上の欠陥、及び入力するまでの経路のチェックをすることができる。

（実施の形態2）

25 本発明の実施の形態2に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムの機密性を保ちながら、該書き換えプログラムが半導体集積回路内の書き換え可能なRAMに正しく格納されているかを確認するために、格納した書き換えプログラムの特定部分のみを半導体集積回路に読み出すように制御する制御回路を備えたものである。

第3図は、本発明の実施の形態2に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

- 図において、300は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、301は制御用マイコン、303はあらかじめ
- 5 暗号化された書き換えプログラムを格納しているメモリ（第1の格納手段）である。半導体集積回路308は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）302と、復号化回路302で復号した書き換えプログラムを格納するための書き換え可能なRAM（第2の格納手段）304と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ307の
- 10 処理を行う演算処理回路（演算処理ユニット）305と、RAM304に格納された書き換えプログラムのうち特定アドレスのみ出力するように制御する制御回路306とから構成される。制御回路306はRAM304の特定のアドレスのみを外部に読み出す機能を有する。

- 次に、以上のように構成された半導体集積回路装置300について、第4図の
- 15 フローチャートを用いて動作を説明する。

- 暗号化された書き換えプログラムを格納するメモリ303からの該書き換えプログラムを復号化回路302で復号し（ステップS401）、該復号化した書き換えプログラムをRAM304に inputs（ステップS402）。次に、制御回路306から、RAM304に格納されている書き換えプログラムの特定アドレスの
- 20 読み出しを行い（ステップS403）、該特定アドレスのプログラムを半導体集積回路308外部に読み出してチェックする（ステップS404）。

- 以上のような本発明の実施の形態2に係る半導体集積回路装置は、書き換えプログラムをRAM304に格納した後、特定のアドレスのみを半導体集積回路外部に読み出すように制御する制御回路を備え、該読み出された特定アドレスを
- 25 チェックすることにより、第三者に漏洩したくない機密情報である書き換えプログラムがRAM304に正しく格納されたかどうかを、該書き換えプログラムの機密性を保持しながら判断することができる。

これは、外部に読み出したのが特定アドレスであっても、それが正しい値であれば、書き換えプログラム全体が正しく格納されていると考えられるからである。

なお、本実施の形態 2 では特定アドレスのみを読み出し可能としたが、特定ビットのみを半導体集積回路外部に読み出すように制御し、該読み出した特定ビットをチェックしても、書き換えプログラムが RAM に格納されたかどうか判断することができる。

5 (実施の形態 3)

本発明の実施の形態 3 に係る半導体集積回路装置は、第三者に漏洩したくない機密情報の書き換えプログラムが半導体集積回路内の書き換え可能な RAM に正しく格納されているかを判断するために、該半導体集積回路の RAM に格納した書き換えプログラムの一部を実行するものである。

- 10 第 5 図は、本発明の実施の形態 3 に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、500 は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、501 は制御用マイコン、503 は、あらかじめ暗号化された書き換えプログラムを格納しているメモリ（第 1 の格納手段）

- 15 である。半導体集積回路 507 は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）502 と、復号化回路 502 で復号化された書き換えプログラムを格納するための書き換え可能な RAM（第 2 の格納手段）504 と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ 506 の処理を行う演算処理回路（演算処理ユニット）505 とから構成される。
- 20

本実施の形態 3 において、上記あらかじめ暗号化された書き換えプログラムには、ダウンロード後に該書き換えプログラムの一部を実行するプログラム（チェックプログラム）が含まれているものとする。また、チェックプログラムは復号化の際に書き換えプログラムに挿入されてもよい。

- 25 次に、以上のように構成された半導体集積回路 500 について、第 6 図のフローチャートを用いてその動作を説明する。

メモリ 503 からの暗号化した書き換えプログラムを復号化回路 502 で復号し（ステップ S601）、該復号した書き換えプログラムを RAM 504 に入力する（ステップ S602）。次に、RAM 504 に格納した書き換えプログラムの一

部を実行させ（ステップS 6 0 3）、正しいか否かが判断されたら、半導体集積回路5 0 7外部に正しいか否かを通知する信号を出力する（ステップS 6 0 4）。

このとき、実行するプログラムの内容を例えばメモリチェックなどのプログラムにし、該メモリチェックを実行させ、そのチェックの結果が得られたならば、

- 5 RAM 5 0 4に正しくプログラムが格納されているかの判断をより確実にできる。

また、第7図のように、実行するプログラムの内容を、JUMP命令などを実行して非連続領域のプログラムを実行するプログラムにし、例えば、先頭プログラムでメモリチェックのプログラムのアドレスXXにJUMPする命令を実行するとする。そして、先頭プログラムからメモリチェックのプログラムのアドレス

- 10 XXにJUMPして、メモリチェックを行うようにすることにより、RAM 5 0 4に正しくプログラムが格納されているかの判断をより確実にできる。また、先頭プログラムで最終プログラムのアドレスYYにJUMPする命令を実行するとする。そして先頭プログラムから最終プログラムのアドレスYYにJUMPして、該最終プログラムは、該最終プログラムを実行後にアドレス0 1に戻るようなプログラムにして、その結果、プログラムが正しく実行されたことを確認することにより、書き換えプログラムがRAMの最後まで書き込まれているかどうかを判断することができ、特に、復号化を1つでも間違えると後段のデータに影響を及ぼす暗号化方式においては、書き換えプログラムが正しく格納されているかをより一層確実に判断できる。

- 20 以上のような本発明の実施の形態3に係る半導体集積回路装置は、書き換えプログラムをRAM 5 0 4に格納した後、該書き換えプログラムの一部を実行し、正しく実行できた場合に信号を出力することによって、書き換えプログラムがRAMに正しく格納できたかどうかを判断することができる。

- 25 また、書き換えプログラムを格納したRAM 5 0 4から、非連続なプログラム領域を順次実行することにより、書き換えプログラムが最後までRAMに正しく格納されたかを確認することが可能になり、RAMに格納した書き換えプログラムの正誤チェックを、より確実に行うことができる。

（実施の形態4）

本発明の実施の形態4に係る半導体集積回路装置は、第三者に漏洩したくない

機密情報である書き換えプログラムが半導体集積回路内に正しく格納されているかを確認するために、半導体集積回路内のRAMに書き換えプログラムを書き込む際に、転送データを監視する転送監視回路を備え、転送されるデータ単位ごとの算術和をとって結果を保持し、チェックサムなどをとるようにしたものである。

- 5 第8図は、本発明の実施の形態4に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

- 図において、801は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、802はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、803は制御用のマイコンである。半導体集積回路810は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）805と、復号化回路805で復号化された書き換えプログラムを格納するためのRAM（第2の格納手段）806と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ807の処理を行う演算処理回路（演算処理ユニット）808と、復号化回路805から転送されるデータ単位ごとの算術和をとる転送監視回路（転送監視手段）809とから構成される。
- 10  
15

次に、本発明の実施の形態4に係る半導体集積回路装置の動作を説明する。

- 以上のように構成された半導体集積回路装置801において、あらかじめ暗号化されメモリ802に格納された書き換えプログラムを、制御用マイコン803の制御のもと、復号化回路805をとおして復号しながらRAM806に格納する。この時、同時に、データ転送用のデータパスの一部である復号化回路805からRAM806への信号線を転送監視回路809が常に監視し、転送されるデータ単位ごとの算術和をとって結果を保持していく。そして、メモリ802に格納されたデータのうちあらかじめ決められたデータ量の転送が終了した時点で、
- 20  
25
- 転送監視回路809に保持されている算術和のデータを読み出し、制御用マイコン803において、あらかじめ計算しておいた正しく転送がおこなわれたときのデータの算術和と比較し、同じ値であれば転送が正しくおこなわれたと判断し、その後、本来実行すべき処理を行う。もし、この両者の値が異なっていれば、正しく転送がおこなわれなかったと判断し、メモリ802に入っているデータを再



度転送し直すなど、しかるべき処置を施す。

- 5 以上のような本発明の実施の形態 4 に係る半導体集積回路装置は、書き換えるための書き換えプログラムの転送データを監視し、転送されるデータ単位ごとの算術和をとる転送監視回路を備え、該転送監視回路でとった算術和と、あらかじめ計算しておいた正しく転送が行われたときのデータの算術和とを比較するので、第三者に漏洩したくない機密情報である書き換えプログラムを読み出すことなく、正しくダウンロードされたか否かを判断することができる。

- 10 なお、本実施の形態 4 では、データ転送監視回路を用いてチェックサムをとる例を説明したが、チェックサムの代わりに CRC チェック回路、ECC チェック回路など、データのあるかたまり単位でビット誤りがあるか否かが判定できるものであれば同様の効果を得ることができ、特にこの監視方式を限定するものではない。

#### (実施の形態 5)

- 15 本発明の実施の形態 5 に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが、半導体集積回路に正しく格納されているか否かを確認するために、演算処理回路のワークメモリから該演算処理回路を動作させることと、RAM に格納されたプログラムデータを演算処理回路に入力させることとを可能にし、演算処理回路にて、チェックサムなどをとるようにしたものである。

- 20 第 9 図は、本発明の実施の形態 5 に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

- 図において、901 は、暗号化された書き換えプログラムをもつ半導体集積回路装置であって、902 はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第 1 の格納手段）であり、903 は制御用のマイコンである。
- 25 半導体集積回路 915 は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）905 と、復号化回路 905 で復号化された書き換えプログラムを格納するための RAM（第 2 の格納手段）906 と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ 907 の処理を行う演算処理回路（演算処理ユニット）908 と、演算処理回路 908 のワークメモリ

- 911と、RAM906、及びワークメモリ911のそれぞれを、演算処理回路908の命令プログラムを読み込むバス913、及びデータを入出力するバス914に接続できるように切り替える接続切り替え回路（接続切り替え手段）912とから構成されている。また、本実施の形態5において、RAM906と演算
- 5 処理回路908の命令プログラムを読み込むバス913とが接続され、ワークメモリ911とデータを入出力するバス914とが接続される形態を第1の形態とし、また、RAM906とデータを入出力するバス914とが接続され、ワークメモリ911と演算処理回路908の命令プログラムを読み込むバス913とが
- 10 接続される形態を第2の形態とし、接続切り替え回路912は、上記第1、及び第2の形態のいずれかの形態に切り替えるものである。通常の状態では、上記第1の形態を取るものとし、これらの構成により、演算処理回路908は、自分自身の命令プログラムを読み込むバス913とデータを読み込むバス914とは独立しているいわゆるハーバードアーキテクチャを取ることができ、より高速にコンテンツデータ907に対するデータ処理が実行できるものである。
- 15 次に、本発明の実施の形態5に係る半導体集積回路装置901の動作を説明する。

- あらかじめ暗号化されメモリ902に格納された書き換えプログラムを制御用マイコン903の制御のもと、復号化回路905をとおして復号しながらRAM906に格納する。その後、演算処理回路908の動作を開始する。このとき演
- 20 算処理回路908は、RAM906の中の書き換えプログラムに組み込まれた実行ステップに応じて動作する。

- また、このRAM906に格納された書き換えプログラムの中に、書き換えプログラムがRAM906に正しく格納できたか否かをチェックするプログラム（チェックプログラム）を予め組み込んでおく。本実施の形態5では、データを
- 25 入出力するバス914上のRAM906のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することによりRAM906に格納されているデータが正しいことを判定するようなプログラムと、正しいと判断された後に接続切り替え回路912を第1の形態に戻すように切り替えるプログラムとの上記2つのプログラムをマシン語データとして組み込んでおき、さらに、

該組み込んだマシン語データを直接ワークメモリ 9 1 1 に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路 9 1 2 を第 2 の形態に切り替えるプログラムとを書き換えプログラムの中に予め組み込んでおく。

- 5     そして、動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ 9 1 1 に展開するプログラムにより、上記マシン語データである、上記 RAM 9 0 6 に格納されたプログラムが正しいか否かを判定するための上記 2 つのプログラムがワークメモリ 9 1 1 に展開される。その後、上記接続切り替え回路 9 1 2 を第 2 の形態に切り替えるプログラムによって、接続切り替
- 10   え回路 9 1 2 を第 2 の形態に切り替える。これにより、ワークメモリ 9 1 1 と、演算処理回路 9 0 8 の命令プログラムを読み込むバス 9 1 3 とが接続されるため、演算処理回路 9 0 8 はワークメモリ 9 1 1 に先ほど展開した上記 2 つのプログラムのうち、データを入出力するバス 9 1 4 上の RAM 9 0 6 のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することにより R
- 15   AM 9 0 6 に格納されているデータが正しいことを判定するようなプログラムを実行する。これにより、RAM 9 0 6 に格納されている書き換えプログラムが正しいと判定されれば、上記ワークメモリ 9 1 1 に展開した 2 つのプログラムの残りのプログラムである、接続切り替え回路 9 1 2 を第 1 の形態に戻すように切り替えるプログラムを実行することによって、接続切り替え回路 9 1 2 は第 1 の形
- 20   態に切り替えられ、以後本来実行すべきプログラムを実行する。

次に、RAM 9 0 6 を第 1 0 図のような構成にした例を説明する。

- この RAM 9 0 6 は、第 1 0 図に示すような論理的構成をとるものである。a 2 4 0 0、a 2 4 0 1、a 2 4 0 2 は、メモリアドレスを示しており、右上がり斜線ハッチをつけたアドレス a 2 4 0 0 で始まり、アドレス a 2 4 0 1 で終わる
- 25   空間に書き換えプログラムを格納する。また、アドレス a 2 4 0 1 で始まり、アドレス a 2 4 0 2 で終わる空間には、上記右上がり斜線ハッチをつけたアドレス a 2 4 0 0 で始まりアドレス a 2 4 0 1 で終わる空間に格納されたデータの、たとえばメモリアドレスごとなどのように、あらかじめ決められた単位ごとに対する、たとえばパリティフラグを格納するものとする。

そして、RAM 906に格納する書き換えプログラムの中にあらかじめ組み込んでおくチェックプログラムとして、データを入出力するバス914上のRAM 906のデータを読み込み、該読み込んだデータの中の1のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムと、さらに前記読み込んだデータに対応するアドレスa2401からa2402の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してメモリ2406に格納された書き換えが正しいか否かを判断するプログラムと、正しいと判断された後に接続切り替え回路912を第1の形態に戻すように切り替えるプログラムとの  
5 上記3つのプログラムをマシン語データとして組み込んでおき、さらに、該組み込んだマシン語データを直接ワークメモリ911に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路912を第2の形態に切り替えるプログラムとを予め組み込んでおく。

動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ911に展開するプログラムにより、上記マシン語データである、上記3つのプログラムがワークメモリ911に展開される。その後、上記接続切り替え回路912を第2の形態に切り替えるプログラムによって、接続切り替え回路912を第2の形態に切り替える。これにより、ワークメモリ911と演算処理回路908の命令プログラムを読み込むバス913とが接続されるため、演算  
15 処理回路908はワークメモリ911に先ほど展開した上記3つのプログラムのうち、データを入出力するバス914上のメモリのデータを読み込み、該読み込んだデータの中の1のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムを実行し、次に、前記読み込んだデータに対応するアドレスa2401からa2402の空間に格納されているパリティ  
20 フラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してRAM 906に格納された書き換えプログラムが正しいか否かを判断するプログラムを実行する。これにより正しいと判断されれば、上記ワークメモリ911に展開した3つのプログラムの残りのプログラムである、接続切り替え回路912を第1の形態に戻すように切り替えるプログラムによつ  
25

て、接続切り替え回路 9 1 2 は第 1 の状態に切り替られ、以後本来実行すべきプログラムを実行する。

このように、RAM 9 0 6 を上記構成にすることにより、RAM 9 0 6 に格納した書き換えプログラムが正しく格納されたか否かを確認することができるととも  
5 もに、書き換えプログラムが正しく格納できていない場合、該正しく格納できていない場所の情報を得ることができる。

なお、RAM 9 0 6 のアドレス a 2 4 0 1 から a 2 4 0 2 までの空間に入れるデータは、パリティフラグに限らず、データのあるかたまりで正しいか否かが判定できるものであればよく、現在よく知られているものに CRC チェックや E C  
10 C チェックなどがあり、これらを使用しても同様の効果が得られる。

以上のような本発明の実施の形態 5 に係る半導体集積回路装置は、RAM 9 0 6 に格納された書き換えプログラムが正しく格納されているかを確認するためのチェックプログラムを演算処理回路のワークメモリ 9 1 1 に展開し、接続切り替え回路 9 1 2 を切り替えて、ワークメモリ 9 1 1 からの命令を可能にし、該ワー  
15 クメモリ 9 1 1 からの命令を受けた演算処理回路にて、チェックサムなどをとることにより、第三者に漏洩したくない機密情報である書き換えプログラムが RAM 9 0 6 に正しく格納されているか否かを、機密性を保持しながら確認することができる。

なお、本発明の実施の形態 5 に係る半導体集積回路装置では、演算処理回路で  
20 チェックサムをとる例を説明したが、チェックサムの代わりに CRC チェック回路、E C C チェック回路など、データのあるかたまり単位でビットに誤りがあるか否かが判定できるものであれば同様の効果を得ることができる。

#### (実施の形態 6)

本発明の実施の形態 6 に係る半導体集積回路装置は、第三者に漏洩したくない  
25 機密情報である書き換えプログラムが半導体集積回路に正しく格納されたか否かの確認を安定して行うために、RAM に格納された書き換えプログラムが正しいか否かの確認をするためのチェックプログラムを予め ROM に格納して、該 ROM に格納したチェックプログラムによって、上記書き換えプログラムの確認動作を行うものである。

第11図は、本発明の実施の形態6に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内にダウンロードする例を示す。

図において、1101は暗号化された書き換えプログラムをもつ半導体集積回路装置であって、1102はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、半導体集積回路1116は、制御用のマイコン1103と、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）1105と、復号化回路1105で復号化した書き換えプログラムを格納するためのRAM（第2の格納手段）1106と、復号化したプログラムの制御手順に従って動作し、コンテンツデータ1107の処理を行う演算処理回路（演算処理ユニット）1108と、演算処理回路1108のワークメモリ1111と、RAM1106、及びワークメモリ1111のそれぞれを、演算処理回路1108の命令プログラムを読み込むバス1113、及びデータを入出力するバス1114に接続できるように切り替える接続切り替え回路（接続切り替え手段）1112と、演算処理回路1108によって実行できるRAM1106に展開された書き換えプログラムが正しいか否かを判定するためのプログラム（チェックプログラム）を格納したROM1115とから構成され、ROM1115は、常に演算処理回路1108の命令プログラムを読み込むバス1113に接続される。また、接続切り替え回路1112によって切り替える第1、及び第2の形態は実施の形態5と同様なので説明を省略する。また、実施の形態5と同様、通常の状態では、上記第1の形態を取るものとする。

次に、本発明の実施の形態6に係る半導体集積回路装置の動作を説明する。

まず最初に、あらかじめ暗号化されメモリ1102に格納された書き換えプログラムを制御用マイコン1103の制御のもと、復号化回路1105をとおして復号しながらRAM1106に格納する。その後、演算処理回路1108の動作を開始する。この時、切り替え回路1112は、第1の形態になるよう接続されているものとする。演算処理回路1108は、RAM1106の中に展開された書き換えプログラムの実行ステップに応じて動作する。この書き換えプログラムの中に、ROM1115の中にあるデータチェック用のプログラムに制御を移す

ようなプログラムがあり、これを実行する。そして、演算処理回路1108の実行プログラムがROM1115に移った後、接続切り替え回路1112を第2の形態になるように切り替える。

5      これにより、RAM1106とデータを入出力するバス1114とが接続されるため、演算処理回路1108は、ROM1115に格納されている、RAM1106に展開された書き換えプログラムが正しいか否かを判断するプログラムに従い、RAM1106のデータを読み込み、かつ正しいかどうかの判断をする。

10      正しいと判断されれば、ROM1115に組み込まれている接続切り替え回路1112を第1の形態に戻すように切り替えるプログラムによって、接続切り替え回路1112は第1の状態に切り替られ、以後本来実行すべきプログラムを実行する。

15      なお、RAM1106に格納されている書き換えプログラムが正しいか否かを確認する方法は、ROM1115に実装されている方式によるが、この方式には、たとえばチェックサムなどが用いられる。しかしながら、必ずしも方式を限定するものではなく、データのある決められた固まり単位で正しいことが判定できればよいことは言うまでもない。

次に、RAM1106を第12図のような構成にした場合について説明する。

第12図は、本発明の実施の形態6に係る半導体集積回路装置のRAM1106の例を示したものである。

20      図において、a2600、a2601、a2602、a2603、a2604は、メモリアドレスを示しており、a2600はRAM1106におけるスタートアドレスを示し、a2604はエンドアドレスを示す。また、右上がり斜線ハッチをつけて示すように、a2601はRAM1106の全容量のちょうど半分に位置する場所のアドレスを示している。また、右下がり斜線をつけて示すように、a2602はアドレスa2601とエンドアドレスa2604とであらわされた容量のちょうど半分

25      に、a2602はアドレスa2601とエンドアドレスa2604とであらわされる容量のちょうど半分に位置するアドレスを示している。

以上のようなRAM1106を用いた半導体集積回路装置1101の動作につ

いて説明する。

まず最初に、RAM 1106のアドレスa 2600からa 2601までの部分にメモリ1102から復号化回路1105を通してデータをダウンロードする。そのあと、アドレスa 2601からa 2604までの領域にも、RAM 1102

5 に格納されている先に展開したアドレスa 2600からa 2601までのデータと全く同じデータを、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路1112を切り替えてRAM 1106のデータを読み出す。この読み出し時に、アドレスa 2600からとアドレスa 2601からのそれぞれの等距離にあるものを順次アクセスし、得られたデータのビットごとの排他的論

10 理和を取る。暗号が正しく解け、データパスに異常がなく、かつ、RAM 1106の格納域ビットに異常がなければ、この排他的論理和の結果は、あるデータと同じデータとの排他的論理和となるため、0になる。したがって、この手順を準次繰り返し、各排他的論理和が0であることを確かめれば、メモリ1102から復号化回路1105を通してRAM 1106に正しく展開できているという判断

15 ができる。上記手順を残り領域の1/2ずつ繰り返し実行することで、RAM 1106には、演算処理回路1108のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

このように、RAM 1106を上記構成にすることにより、何らかの不具合のために、上記手順の排他的論理和が0とならない場合には、RAM 1106に格納されているデータに不具合があると判断できるとともに、不具合発生アドレス

20 も知ることができる。

なお、メモリ1102からRAM 1106に展開するデータ量は、RAM 1106の書き換えプログラムが格納されていない領域の1/2以下ずつであればよいが、排他的論理和をとる上記方法においては、1/2が読み出し可能な最大データ量であるので、1/2とすることで書き込み効率を大きくとれる。

25

また、本実施の形態6において、このように構成されたRAM 1106を用いて、データチェックプログラムROM 1115に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムROM 1115がない場合でも、実施の形態5のように、ダウンロードするプログラムに予



めデータチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

次に、メモリ 1102 の構成を第 13 図のような構成にした場合について説明する。

- 5 第 13 図は、本発明の実施の形態 6 に係る半導体集積回路装置におけるメモリ 1102 の例を示したものである。

- 図において、a2710、a2711、a2712、a2713、a2714、a2715、a2716、a2717 は、メモリ 1102 におけるアドレスを示している。アドレス a2710 は、メモリ 1102 のスタートアドレスを示し、
- 10 アドレス a2717 は、メモリ 1102 のエンドアドレスを示す。また、アドレス a2710 とアドレス a2711 に囲まれた空間には、第 12 図で示した RAM1106 のアドレス a2600 から a2601 に入るべきデータを暗号化して格納する。便宜上これを「データ A」と呼ぶ。また、アドレス a2711 とアドレス a2712 に囲まれた空間には、復号化回路 1105 によって復号化すると
- 15 RAM1106 のアドレス a2600 から a2601 に入るべきデータ、即ち「データ A」を各ビットごとに反転したものが得られるようなデータが格納される。これを便宜上「データ A<sup>′</sup>」と呼ぶ。同様に、アドレス a2712 とアドレス a2713 に囲まれた空間には、RAM1106 のアドレス a2601 から a2602 に入るべきデータを暗号化したものを格納し、アドレス a2713 とアドレス
- 20 a2714 に囲まれた空間には、復号化回路 1105 によって復号化すると RAM1106 のアドレス a2601 から a2602 に入るべきデータを各ビットごとに反転したものが得られるようなデータが格納される。これらを便宜上それぞれ、「データ B」「データ B<sup>′</sup>」と呼ぶ。「データ C」及び「データ C<sup>′</sup>」も同様の対応である。このような手順を繰り返し、RAM1106 に格納すべき全ての
- 25 プログラム及びその反転データを上記手順に従って、暗号化してメモリ 1102 に格納する。

以上のように構成されたメモリ 1102、及び RAM1106 を使った半導体集積回路装置 1101 の動作について説明する。

まず、RAM1106 のアドレス a2600 から a2601 までの部分にメモ

- り1102から復号化回路1105を通して「データA」をダウンロードする。そのあと、上記手順にて述べたメモリ1102に格納されている今ダウンロードしたデータの反転データを暗号化したものである「データA<sup>′</sup>」を、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路1112を切り
- 5 替えてRAM1106のデータを読み出す。この読み出し時に、アドレスa2600からとアドレスa2601からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの論理積を取る。暗号が正しく解け、データパスに異常がなく、かつ、RAM1106の格納域ビットに異常がなければ、この論理積の結果は、あるデータとその反転データとの論理積となるため、0になる。
- 10 る。したがって、この手順を順次繰り返し、各論理積が0であることをたしかめれば、メモリ1102から復号化回路1105を通してRAM1106に正しく展開できているということになる。メモリ1102には、RAM1106の各手順における残りの領域の1/2ずつのデータとその反転データが暗号化されて「データB」「データB<sup>′</sup>」「データC」「データC<sup>′</sup>」などのように対になって
- 15 必要な量だけ格納されており、上記手順を残り領域の1/2ずつデータがなくなるまで繰り返し実行することで、RAM1106には、演算処理回路1108のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

- これにより、もしも何らかの不具合のために、上記手順の論理積が0とならない場合に、RAM1106に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。また、何らかの理由により、復号化回路1105に不具合がありRAM1106への出力が固定値になっていても、RAM2506に格納されているデータを上記手順で論理積をとれば、あるデータと同じデータの論理積であるため、0にはならない。このことで、正しく
- 25 ぐデータが格納されてはいないと判断できる。

なお、メモリ1102からRAM1106に展開するデータ量は、該RAM1106の残り領域の1/2以下ずつであってもよいが、論理積をとる上記方法においてはRAM1106の残り領域の1/2が読み出し可能な最大データ量であるので、1/2とすることで書き込み効率を大きくとれる。

また、本実施の形態6において、このように構成されたメモリ1102を用いて、データチェックプログラムROM1115に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムROM1115がない場合でも、実施の形態5のように、ダウンロードする書き換えプログラムに予めチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

以上のような本発明の実施の形態6に係る半導体集積回路装置は、RAM1106に格納されている書き換えプログラムが正しく格納されているか否かを確認するためのチェックプログラムをROM化したメモリ1115に格納したので、  
10 チェックプログラムの転送や、展開に誤りが発生しても、RAM1106に格納された書き換えプログラムが正しく格納できたか否かの確認を、容易に、かつ、安定して行うことができる。

また、RAM1106の書き換えプログラムが格納されていない領域を2分割した各々の領域に、該書き換えプログラムが格納されていない領域の1/2に相当するプログラムデータと、該1/2の領域に読み出したプログラムデータと同じデータとを順次読み出し、該読み出したそれぞれのデータから排他的論理和をとる手順を繰り返し行うようにしたので、RAM1106に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、書き換えプログラムがRAM1106に正しく格納できていない場合に、RAM1106に  
20 おける正しく格納できていない場所の情報を得ることができる。

また、RAM1106の書き換えプログラムが格納されていない領域を2分割した各々の領域に、該書き換えプログラムが格納されていない領域の1/2に相当するプログラムデータと、該1/2の領域に読み出したプログラムデータを反転したデータとを順次読み出し、該読み出したそれぞれのデータから論理積をとる手順を繰り返し行うようにしたので、RAM1106に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、何らかの理由により復号化回路1105の不具合でRAM1106への出力が固定値になり、排他的論理和をとってもデータが一致し、上記第2の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、R

AM1106に格納したプログラムの正誤を正しく判別できる。

なお、本発明の実施の形態1～6に係る半導体集積回路装置では、予め暗号化した書き換えプログラムを、半導体集積回路内にダウンロードする例を説明したが、暗号化されていない書き換えプログラムを半導体集積回路内にダウンロード

5 しても同様の効果が得られるのはいうまでもない。

(実施の形態7)

本発明の実施の形態7に係る半導体集積回路装置は、予め暗号化された書き換えプログラムをメモリに格納した半導体集積回路装置において、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納されたか否かを、該書き換えプログラムの機密性を保持しながら確認するために、上記暗号化された書き換えプログラムを復号してRAMに格納した後、該書き換えプログラムを再度暗号化し、該再度暗号化したプログラムデータと、上記予め暗号化されたプログラムデータとを比較するようにしたものである。

15 第14図は、本発明の実施の形態7に係る半導体集積回路装置の構成を示す図である。

図において、1401は暗号化された書き換えプログラムをもつ半導体集積回路装置であり、1402はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、1403は制御用のマイコンである。半導体集積回路1411は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）1405と、復号化回路で復号された書き換えプログラムを格納するためのRAM（第2の格納手段）1406と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ1407の処理を行う演算処理回路（演算処理ユニット）1408と、上記RAM1406に転送されたデータを再度暗号化する暗号化回路（暗号化手段）1410とから構成される。

25 次に、以上のように構成された半導体集積回路装置1401の動作を説明する。

まず、あらかじめ暗号化されメモリ1402に格納された書き換えプログラムを制御用マイコン1403の制御のもと、復号化回路1405をとおして復号しながらRAM1406に格納する。そして、メモリ1402に格納されたデータのうち、あらかじめ決められたデータ量の転送が終了した時点で、今度は、制御

用マイコン1403の制御のもと、今復号化してメモリ1406に格納した書き換えプログラムを読み出し、暗号化回路1410を通して再度暗号化し、該再度暗号化したプログラムデータとメモリ1402に格納されている予め暗号化したプログラムデータとを比較する。この両者のデータが一致すれば、最初にメモリ

5 1402から読み出し、復号化回路1405にて復号化し、RAM1406に格納した書き換えプログラムが、正しいと判断できる。

以上のような、本発明の実施の形態7に係る半導体集積回路装置は、予め暗号化したプログラムを半導体集積回路1411にダウンロードする半導体集積回路装置において、暗号化した書き換えプログラムを復号化し、RAM1406に格

10 納した後、暗号化回路1410で再度暗号化し、予め暗号化した書き換えプログラムと再度暗号化した書き換えプログラムとを比較するようにしたので、第三者に漏洩したくない機密情報の書き換えプログラムをそのまま外部に読み出すことなく、RAM1406に格納した書き換えプログラムが正しく格納できたか否かを確認することができる。

15 (実施の形態8)

本発明の実施の形態8に係る半導体集積回路装置は、RAMに格納した書き換えプログラムが正しくないと判定された場合、該書き換えプログラムの修正箇所を検出して書き換えプログラムを修正可能にしたものである。

以下、本発明の実施の形態8に係る半導体集積回路装置を、第15図、第16

20 図、及び第17図を用いて説明する。

第15図は、本発明の実施の形態8に係る半導体集積回路装置の構成を示した図であり、実施の形態7で説明した半導体集積回路装置において、RAMに格納されたプログラムが正しくないと判断された場合、プログラムを修正可能とする例を示したものである。

25 図において、1500は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、1503はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、1501は制御用のマイコンである。半導体集積回路1509は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）1502と、復号化回路1

502で復号された書き換えプログラムを格納するためのRAM（第2の格納手段）1504と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ1508の処理を行う演算処理回路（演算処理ユニット）1505と、RAM1504に格納された書き換えプログラムを再度暗号化する暗号化回路1506とから構成される。ここまでの構成は第14図の半導体集積回路装置1401と同じであるが、半導体集積回路装置1500においては、暗号化回路1506の出力S1506とあらかじめ暗号化された書き換えプログラムが格納されているメモリ1503の出力S1503とを比較し、RAM1504に正しく格納されなかった場所を検出する比較器1507を備えている。

- 10    以上のように構成された半導体集積回路装置1500について、以下にその動作を説明する。第16図は、実施の形態8に係る半導体回路1500の動作フローを示す。

まず、暗号化した書き換えプログラムを復号化回路1502で復号し（ステップS1601）、制御用マイコン1501にしたがい、復号化した書き換えプログラムをRAM1504に入力する（ステップS1602）。ステップS1602でRAM1504に入力した書き換えプログラムを暗号化回路1506で再度、暗号化し（ステップS1603）、ステップS1603で暗号化した書き換えプログラムとメモリ1503に保持している書き換えプログラムとを比較する（ステップS1604）。ステップS1604でのチェックで正しくない場合、制御用マイコン1501に従って、正しくない部分のRAMのビットを使用しないように書き換えプログラムを修正する（ステップS1605）。そして、ステップS1605で修正したプログラムを復号化し（ステップS1606）、該復号化したプログラムをRAM1504に入力する（ステップS1607）。

25    また、ステップS1605の書き換えプログラム修正の動作は、例えば、第17図のように、RAM1504に格納された書き換えプログラムの正しくない部分が、例えばマシン語単位などあらかじめ決められた単位のアドレスXXからアドレスXX'とすると、アドレスXXからアドレスXX'に格納されるべきデータを修正プログラムとしてアドレスYYからアドレスYY'に格納するようにする。このとき、修正プログラムに、アドレスXXまで読み出したときにアドレ

スYYにJUMPする命令プログラムと、次にアドレスYY´まで読み出したときにアドレスXX´にJUMPする命令プログラムとを組み込むように修正を行えばよく、このように修正を行うことにより、RAM1504に格納されたプログラムの読み出しを正常に行うことができる。

- 5      これにより、上記方法によると、修正プログラムをRAM1504に入力した後、読み出してチェックすることによりRAM1504内の欠陥のあるビットを使わないようにできるため、RAMの有効活用ができる。

- 10      なお、本実施の形態8では、予め暗号化した書き換えプログラムを格納するメモリ1503からの出力S1503と復号した書き換えプログラムを再度暗号化する暗号化回路1506からの出力S1506とを比較した結果から、RAM1504に正しく格納できなかった場所を検出して、書き換えプログラムを修正したが、上述した書き換えプログラムの修正は、RAMの欠陥位置を検出できれば可能であるので、実施の形態6で説明したメモリ、及びRAMの構成により読み出したデータの排他的論理和、及び論理積をとってデータをチェックする例において適用可能である。

- 15      以上のような、実施の形態8に係る半導体集積回路装置は、書き換えプログラムがRAMに正しく格納されたか否かを確認した結果、RAMに正しく格納されなかった場合に、正しく書き込めていないRAMのビットを使用しないように書き換えプログラムを修正して、RAMにダウンロードするので、RAMの一部のビットが正しく生成できていなくても、その他の部分に書き込んで、書き換えプログラムを正しく動作させることができ、RAMを有効に活用することができる。

- 20      なお、本発明の実施の形態1～8の半導体集積回路装置では、書き換えプログラムをメモリ（第1の格納手段）に格納して、半導体集積回路内にダウンロードしたが、半導体集積回路装置外部に書き換えプログラムを保持し、例えば、インターネット等の通信手段を用いて、半導体集積回路内にダウンロードしても同様の効果を得ることができるのはいうまでもない。

25      また、本発明の実施の形態1～8では、半導体集積回路装置を例にとって説明したが、半導体集積回路装置に相当するものが、外部からアクセス不可能な領域（格納手段）を有する半導体集積回路を搭載したシステムであってもよく、該シ

システムのアクセス不可能な領域（格納手段）に対し機密データのダウンロードが成功したか否かを検証するデータ記憶検証装置（方法）であってもよく、同様の効果を得ることができるのはいうまでもない。

- また、本発明の実施の形態 2 ～ 8 の半導体集積回路装置では、プログラムを格納する R A M は外部からの読み出しが不可のものであることはいうまでもない。
- 5

#### 産業上の利用可能性

- 以上のように、本発明にかかる半導体集積回路装置、データ記憶検証装置およびデータ記憶検証方法は、機密性を要するプログラムデータを外部に漏らすことなく、正しく半導体集積回路内にダウンロードできたか否かを確認でき、特に著作権保護が必要なプログラム等のダウンロードが成功したか否かを確認するのに適する。
- 10



## 請求の範囲

1. 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

- 10 上記第2の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、

- 上記第2の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第1の格納手段からの上記書き換えプログラムを、上記第2の格納手段の外部読出し不可能領域に格納するようにした、
- 15

ことを特徴とする半導体集積回路装置。

2. 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、
- 20

上記第2の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えた、

- 25 ことを特徴とする半導体集積回路装置。

3. 請求の範囲第2項に記載の半導体集積回路装置において、

上記制御回路は、上記第2の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

4. 請求の範囲第2項に記載の半導体集積回路装置において、  
上記制御回路は、上記第2の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとした、  
ことを特徴とする半導体集積回路装置。
- 5 5. 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、  
上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、  
上記第2の格納手段に格納した上記書き換えプログラムの一部を実行する、  
ことを特徴とする半導体集積回路装置。
- 10 6. 請求の範囲第5項に記載の半導体集積回路装置において、  
上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである、  
ことを特徴とする半導体集積回路装置。
- 20 7. 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、  
上記半導体集積回路内に、上記第1の格納手段から上記第2の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えた、  
ことを特徴とする半導体集積回路装置。
- 25 8. 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回

路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

- 5      上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、

        上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、

        上記第2の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、

- 10      上記第2の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行う、

        ことを特徴とする半導体集積回路装置。

- 15      9.      請求の範囲第8項に記載の半導体集積回路装置において、

        上記第2の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとした、

        ことを特徴とする半導体集積回路装置。

- 20      10.      請求の範囲第9項に記載の半導体集積回路装置において、

        上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用する、

        ことを特徴とする半導体集積回路装置。

11.      請求の範囲第8項に記載の半導体集積回路装置において、

- 25      上記第2の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次2分割した構成とし、該2分割した各々の領域に同じプログラムデータを格納するものであり、

        上記チェックプログラムは、上記2分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、

前回の判定結果が正しいと判定されたときに、前回 2 分割した領域の一方の領域を、プログラムが格納されていない領域としてさらに 2 分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、  
上記第 2 の格納手段に格納すべきプログラムすべてを順次格納する、

5      ことを特徴とする半導体集積回路装置。

1 2.    請求の範囲第 1 1 項に記載の半導体集積回路装置において、

上記第 2 の格納手段は、該第 2 の格納手段の上記書き換えプログラムが格納されていない領域を順次 2 分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとした、

10      ことを特徴とする半導体集積回路装置。

1 3.    請求の範囲第 1 2 項に記載の半導体集積回路装置において、

上記一意に得られるデータが、該プログラムデータの反転データである、  
ことを特徴とする半導体集積回路装置。

15      1 4.    請求の範囲第 8 項ないし 1 3 のいずれかに記載の半導体集積回路装置において、

上記チェックプログラムを予め格納した R O M (Read Only Memory) を備え、  
上記 R O M により上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行う、

20      ことを特徴とした半導体集積回路装置。

1 5.    請求の範囲第 1 項ないし第 1 4 項のいずれかに記載の半導体集積回路装置において、

上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、

25      上記第 1 の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第 2 の格納手段に復号化した上記書き換えプログラムを格納する、

ことを特徴とする半導体集積回路装置。

1 6.    半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさ

せるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第1の格納手段を用いて書き換えを

5 行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第1の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第2の格納手段に転送する復号化手段と、

10 上記第2の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、

上記暗号化手段で暗号化された書き換えプログラムと上記第1の格納手段に保持している暗号化された書き換えプログラムとを比較する、

ことを特徴とする半導体集積回路装置。

15 17. 請求の範囲第11項ないし第13項、及び第16項のいずれかに記載の半導体集積回路装置において、

上記第2の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第1の格納手段に保持した書き換えプログラムを修正可能とした、

ことを特徴とする半導体集積回路装置。

20 18. 請求の範囲第1項ないし第17項のいずれかに記載の半導体集積回路装置において、

当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能とした、

ことを特徴とする半導体集積回路装置。

25 19. 任意のデータを外部からアクセス可能な領域に記憶させる手段と、前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する手段と、正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能な領域に記憶させる手段とを備えた、

ことを特徴とするデータ記憶検証装置。

20. 機密データを外部からアクセス不可能な領域に記憶させる手段と、

前記機密データの特定部分を外部に出力する手段とを備えた、  
ことを特徴とするデータ記憶検証装置。

2 1. プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる手段と、

5 前記記憶されたプログラムを実行させ、結果を外部に出力する手段とを備えた、  
ことを特徴とするデータ記憶検証装置。

2 2. 検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第 1 の手段と、

前記検査プログラムを実行させ、結果を外部に出力する第 2 の手段と、

10 前記第 2 の手段の終了後、前記機密プログラムを実行させる第 3 の手段とを備えた、  
ことを特徴とするデータ記憶検証装置。

2 3. 機密データを外部からアクセス不可能な領域に記憶させる手段と、  
前記記憶させると同時に前記機密データを用いて所定の演算を行う手段と、

15 前記演算の結果を外部に出力する手段とを備えた、  
ことを特徴とするデータ記憶検証装置。

2 4. 機密データを外部からアクセス不可能な第 1 の領域に記憶させる第 4 の手段と、

20 機密データの一部であり、前記第 1 の領域に記憶されている検査プログラムを第 2 の領域に記憶させる第 5 の手段と、

前記第 2 の領域に記憶されている検査プログラムを実行して、前記第 1 の領域の機密データの正当性を検査する第 6 の手段とを備えた、  
ことを特徴とするデータ記憶検証装置。

2 5. 請求項 2 4 記載のデータ記憶検証装置において、

25 前記第 6 の手段の終了後に前記第 1 の領域の命令に制御を移す第 7 の手段をさらに備えた、

ことを特徴とするデータ記憶検証装置。

2 6. 請求項 2 4 記載のデータ記憶検証装置において、

前記第 5 の手段は、前記第 1 の領域に記憶されている機密データ内に存在する

命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

27. 請求項24記載のデータ記憶検証装置において、

前記第5の手段は、第3の領域に前記第4の手段による記憶の実行以前に記憶

5 された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証装置。

28. 機密データを復号する手段と、

前記復号されたデータを外部からアクセス不可能な領域に記憶させる手段と、

前記記憶されたデータを暗号化する手段と、

10 前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータ  
が正しく記憶されたか否かを判定する手段とを備えた、

ことを特徴とするデータ記憶検証装置。

29. 機密プログラムを外部からアクセス不可能な領域に記憶させる第21の  
手段と、

15 前記記憶されたプログラムを読み出す第22の手段と、

前記読み出されたプログラムを命令単位で正当性を判定する第23の手段と、

正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可  
能な領域において空いている領域に記憶させる第24の手段と、

前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次の

20 アドレスにジャンプする命令を記憶させる第25の手段と、

正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャン  
プする命令を記憶させる第26の手段とを備えた、

ことを特徴とするデータ記憶検証装置。

30. 任意のデータを外部からアクセス可能な領域に記憶させる工程と、

25 前記任意のデータを外部に出力し、正しく記憶されたか否かを判定する工程と、

正しく記憶されたと判定された場合は、機密データを外部からアクセス不可能  
な領域に記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

31. 機密データを外部からアクセス不可能な領域に記憶させる工程と、

前記機密データの特定部分を外部に出力する工程とを含む、  
ことを特徴とするデータ記憶検証方法。

3 2. プログラムを含んだ機密データを外部からアクセス不可能な領域に記憶させる工程と、

5 前記記憶されたプログラムを実行させ、結果を外部に出力する工程とを含む、  
ことを特徴とするデータ記憶検証方法。

3 3. 検査プログラムと機密プログラムとを含む機密データを外部からアクセス不可能な領域に記憶させる第1の工程と、

前記検査プログラムを実行させ、結果を外部に出力する第2の工程と、

10 前記第2の工程の終了後、前記機密プログラムを実行させる第3の工程とを含む、

ことを特徴とするデータ記憶検証方法。

3 4. 機密データを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶させると同時に前記機密データを用いて所定の演算を行う工程と、

15 前記演算の結果を外部に出力する工程とを含む、

ことを特徴とするデータ記憶検証方法。

3 5. 機密データを外部からアクセス不可能な第1の領域に記憶させる第4の工程と、

20 機密データの一部であり、前記第1の領域に記憶されている検査プログラムを第2の領域に記憶させる第5の工程と、

前記第2の領域に記憶されている検査プログラムを実行して、前記第1の領域の機密データの正当性を検査する第6の工程とを含む、

ことを特徴とするデータ記憶検証方法。

3 6. 請求項3 6記載のデータ記憶検証方法において、

25 前記第6の工程の終了後に前記第1の領域の命令に制御を移す第7の工程をさらに含む、

ことを特徴とするデータ記憶検証方法。

3 7. 請求項3 5記載のデータ記憶検証方法において、

前記第5の工程は、前記第1の領域に記憶されている機密データ内に存在する



命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

38. 請求項35記載のデータ記憶検証方法において、

前記第5の工程は、前記第3の領域に前記第4の工程による記憶の実行以前に

5 記憶された命令により前記検査プログラムの記憶を実行する、

ことを特徴とするデータ記憶検証方法。

39. 機密データを復号する工程と、

前記復号されたデータを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶されたデータを暗号化する工程と、

10 前記暗号化されたデータと前記機密データとを比較して前記記憶されたデータ  
が正しく記憶されたか否かを判定する工程とを含む、

ことを特徴とするデータ記憶検証方法。

40. 機密プログラムを外部からアクセス不可能な領域に記憶させる工程と、

前記記憶されたプログラムを読み出す工程と、

15 前記読み出されたプログラムを命令単位で正当性を判定する工程と、

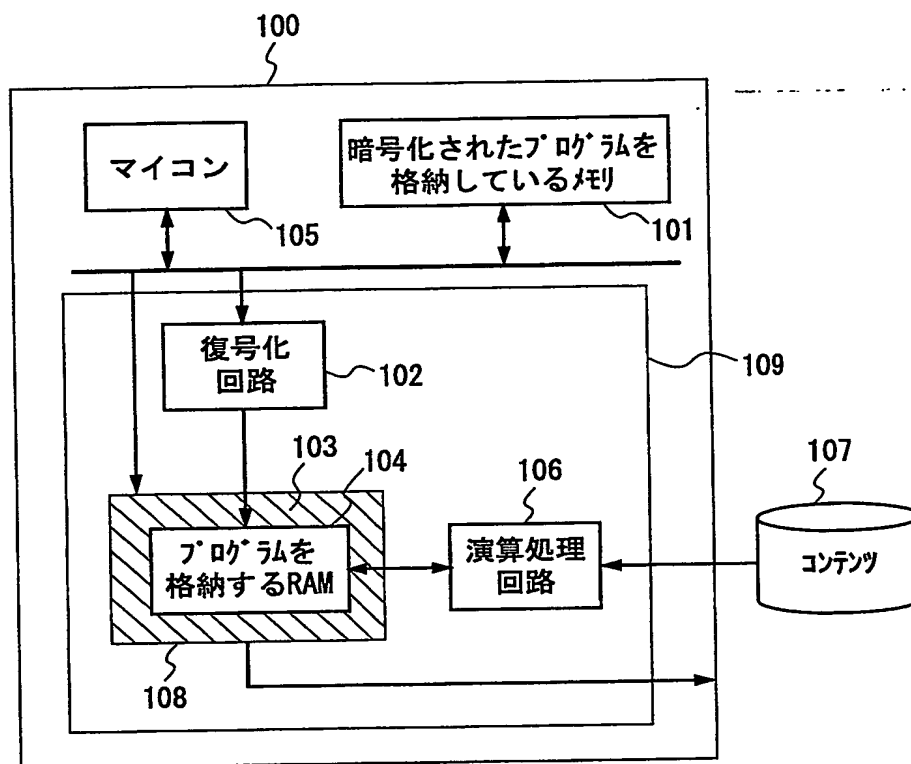
正当でないと判定された場合は、正当な命令を再度前記外部からアクセス不可  
能な領域において空いている領域に記憶させる工程と、

前記再度記憶された命令の次の命令を正当でないと判定されたアドレスの次の  
アドレスにジャンプする命令を記憶させる工程と、

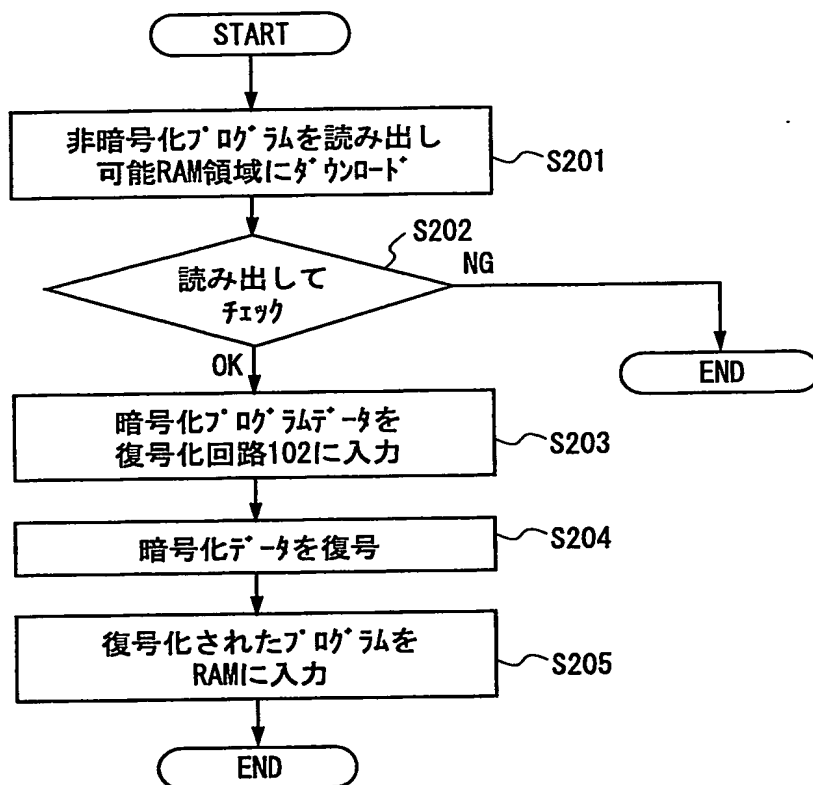
20 正当でないと判定された領域には、前記再度記憶された命令のアドレスにジャン  
プする命令を記憶させる工程とを含む、

ことを特徴とするデータ記憶検証方法。

第1図

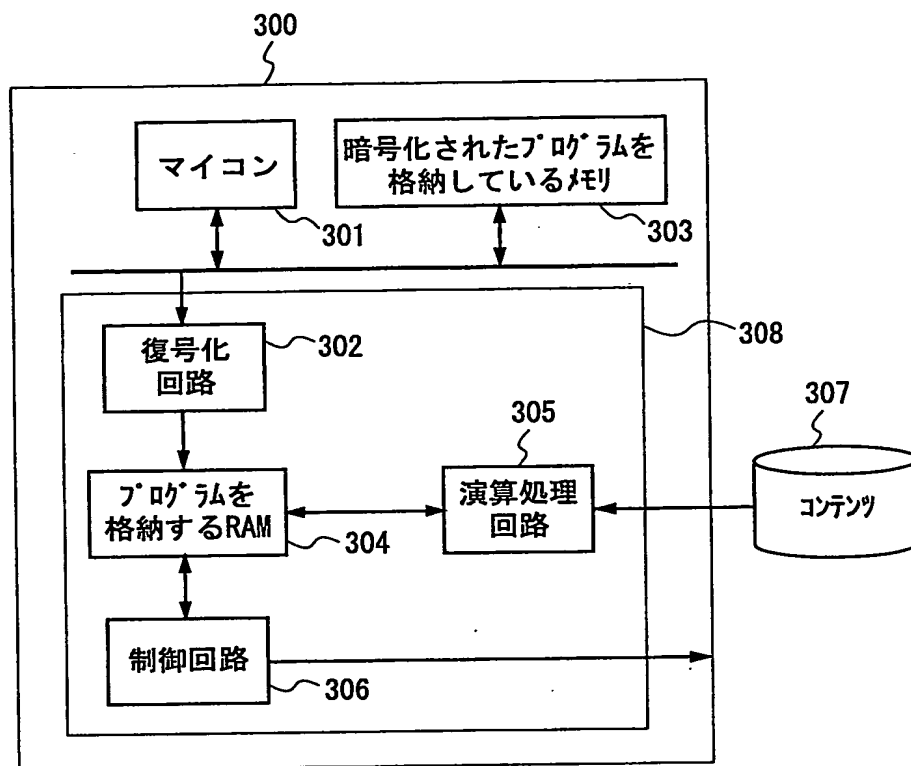


第2図

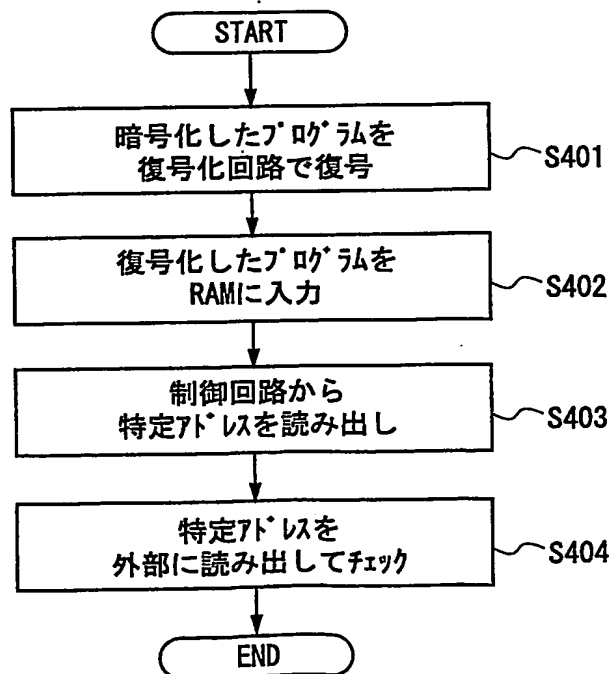


3/12

第3図

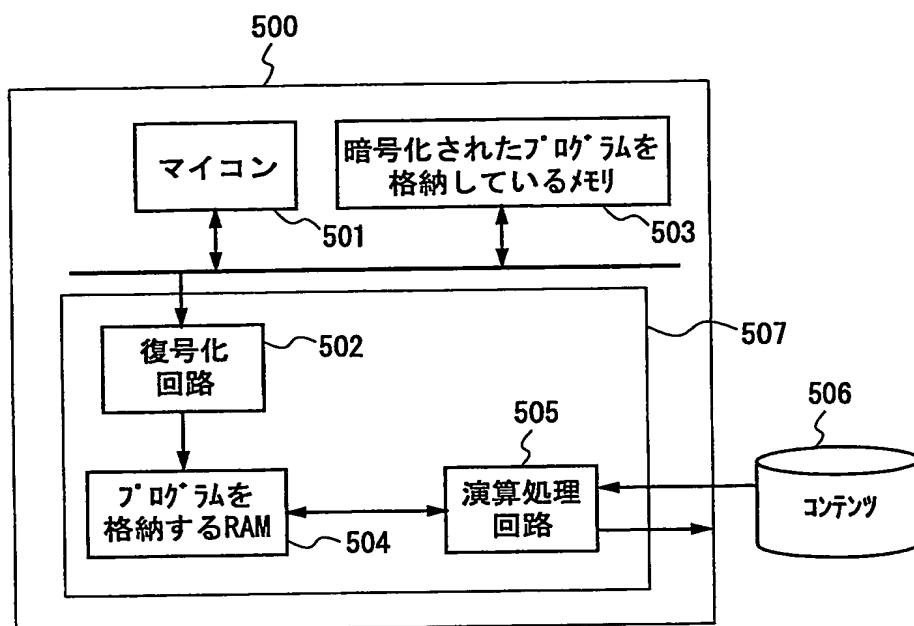


第4図

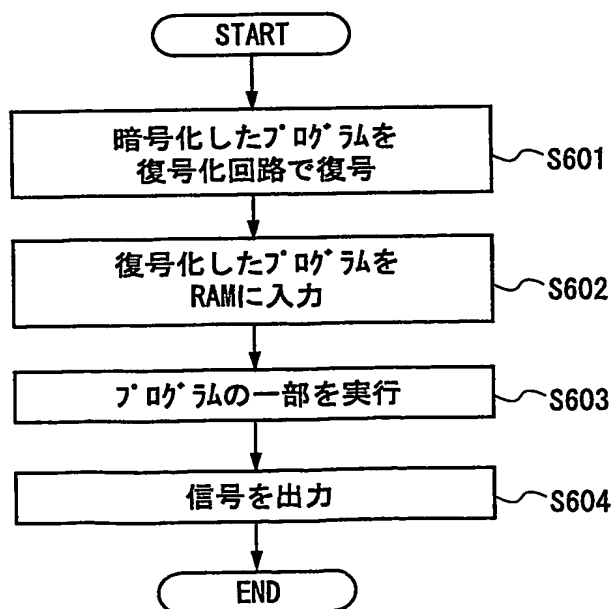


4/12

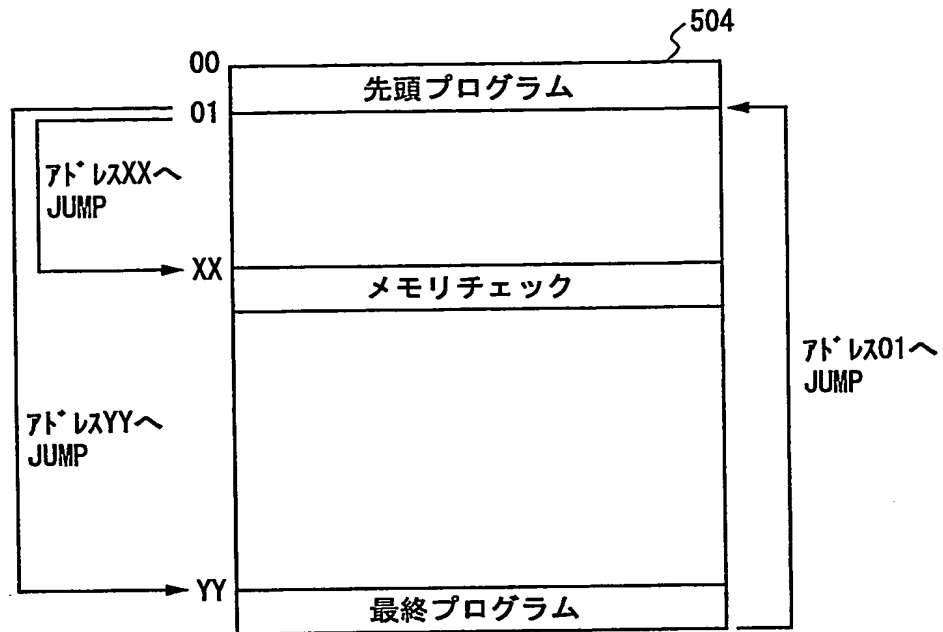
第5図



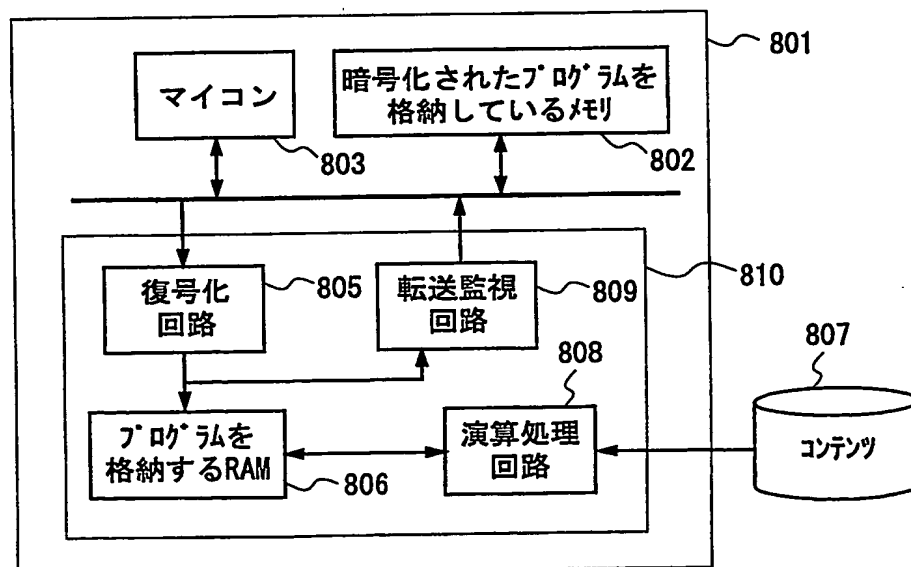
第6図



第7図

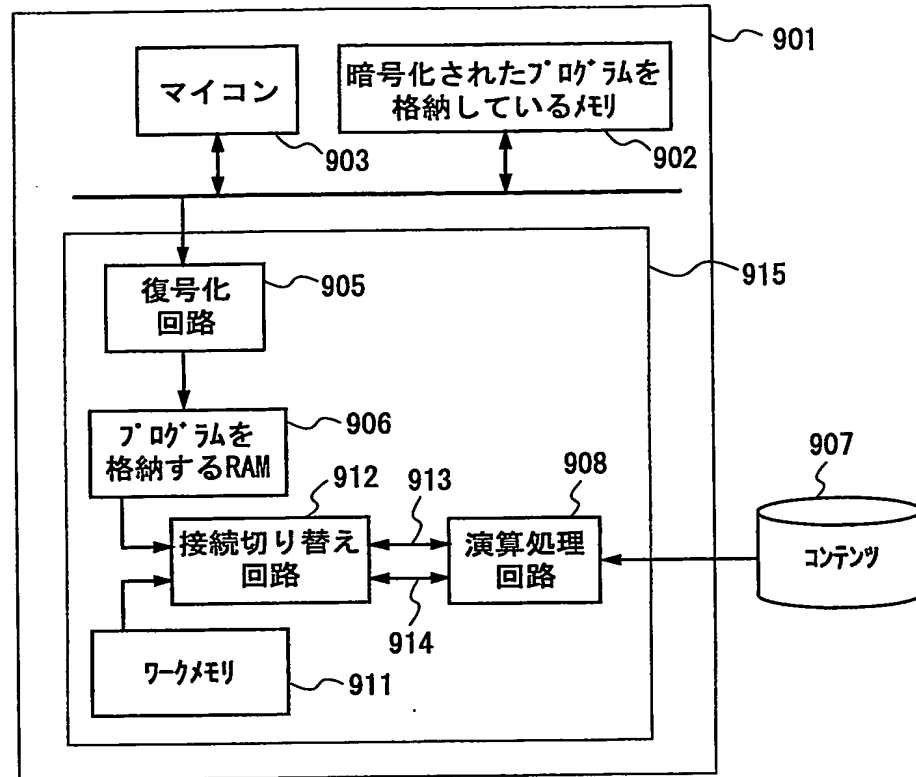


第8図

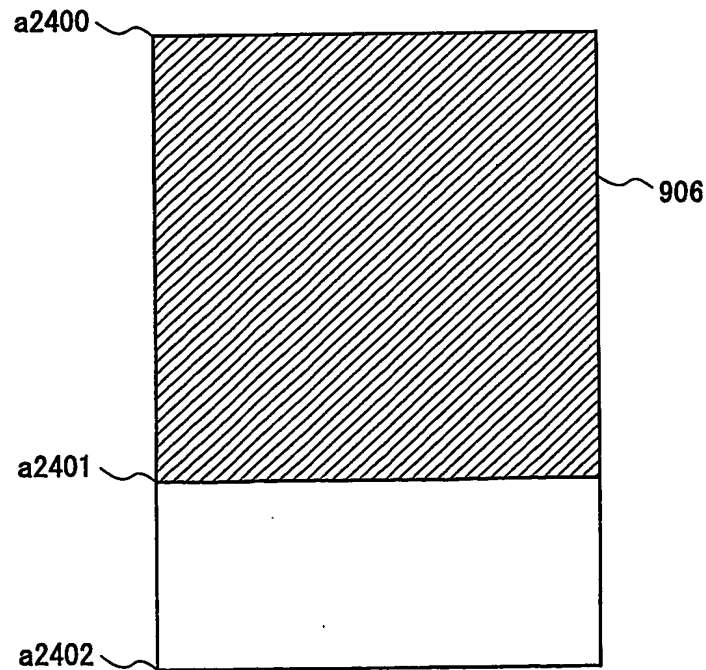


6/12

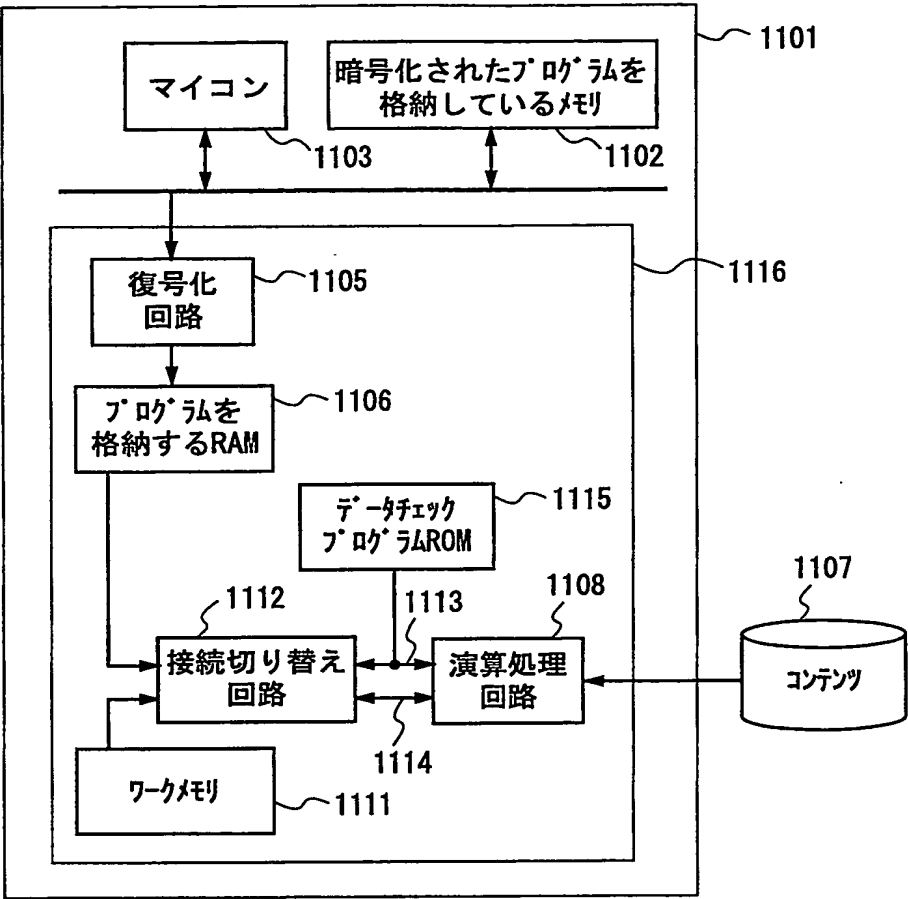
第9図



第10図

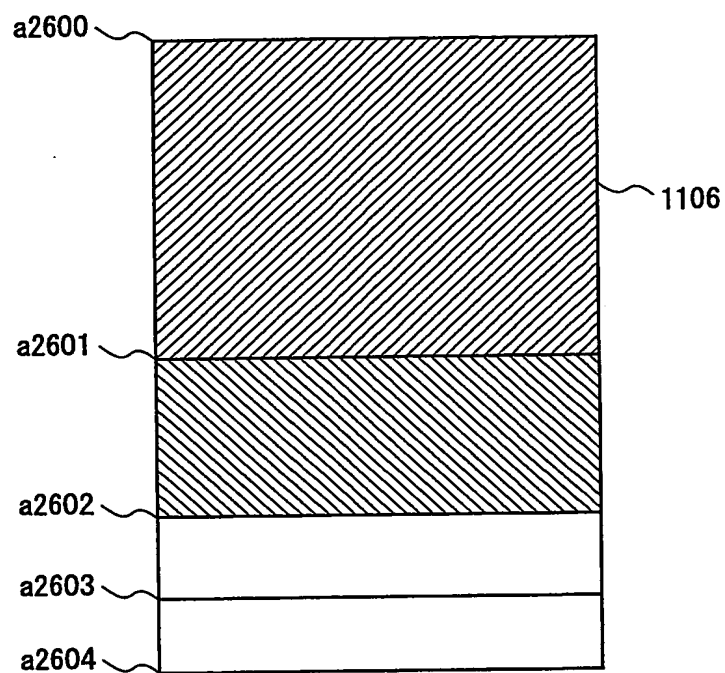


第11図

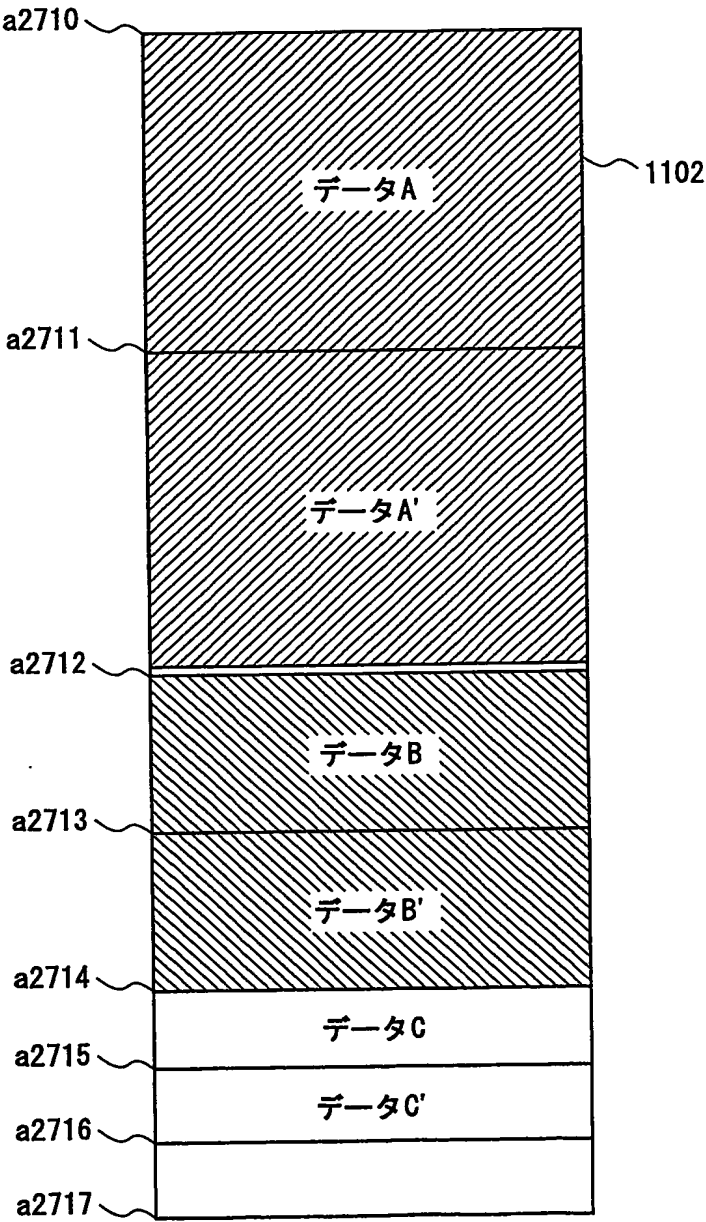




第12図

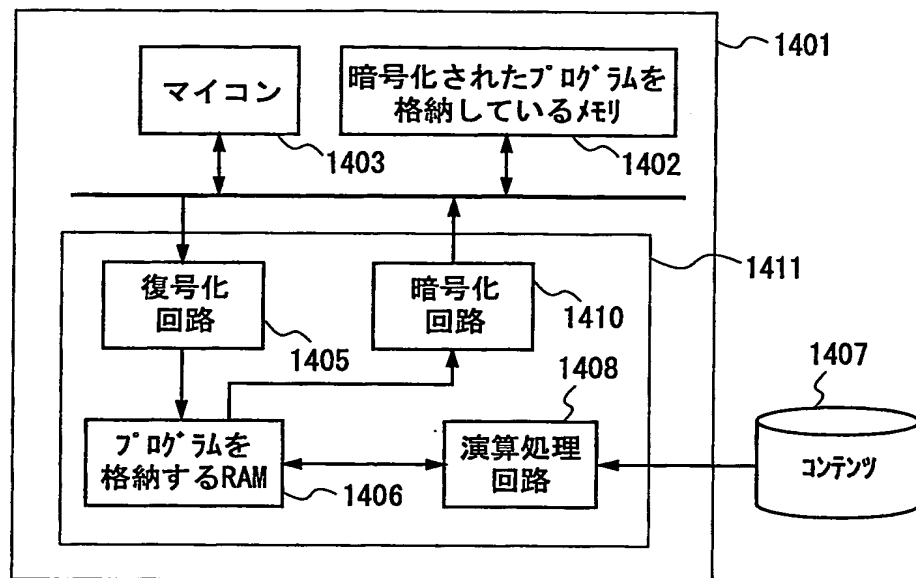


第13図

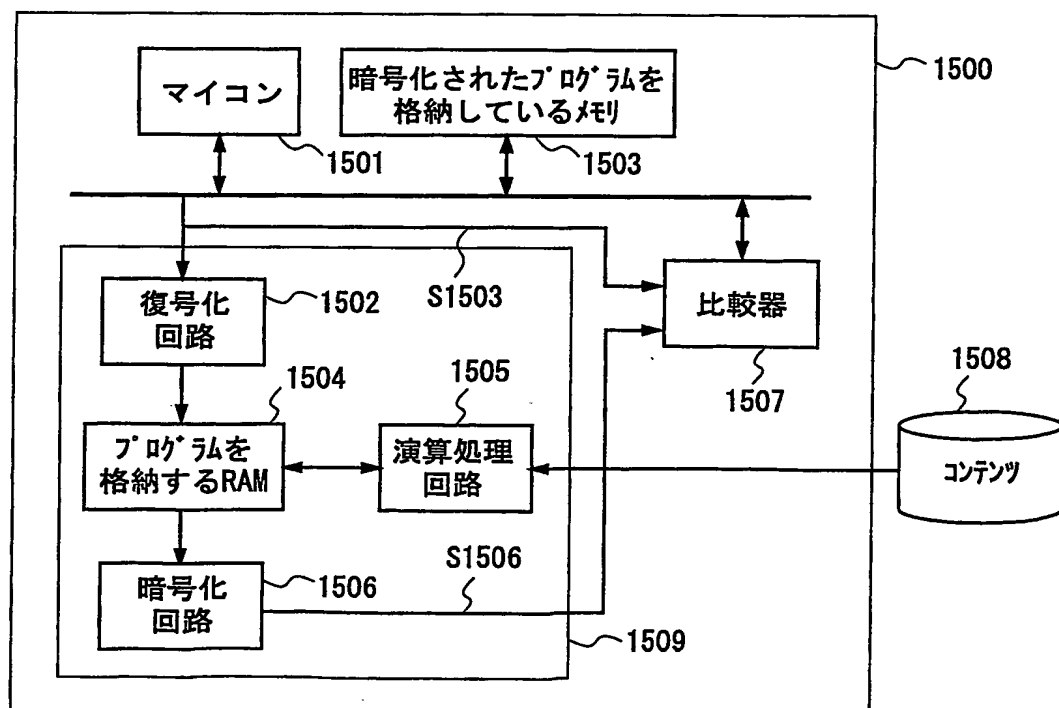


10/12

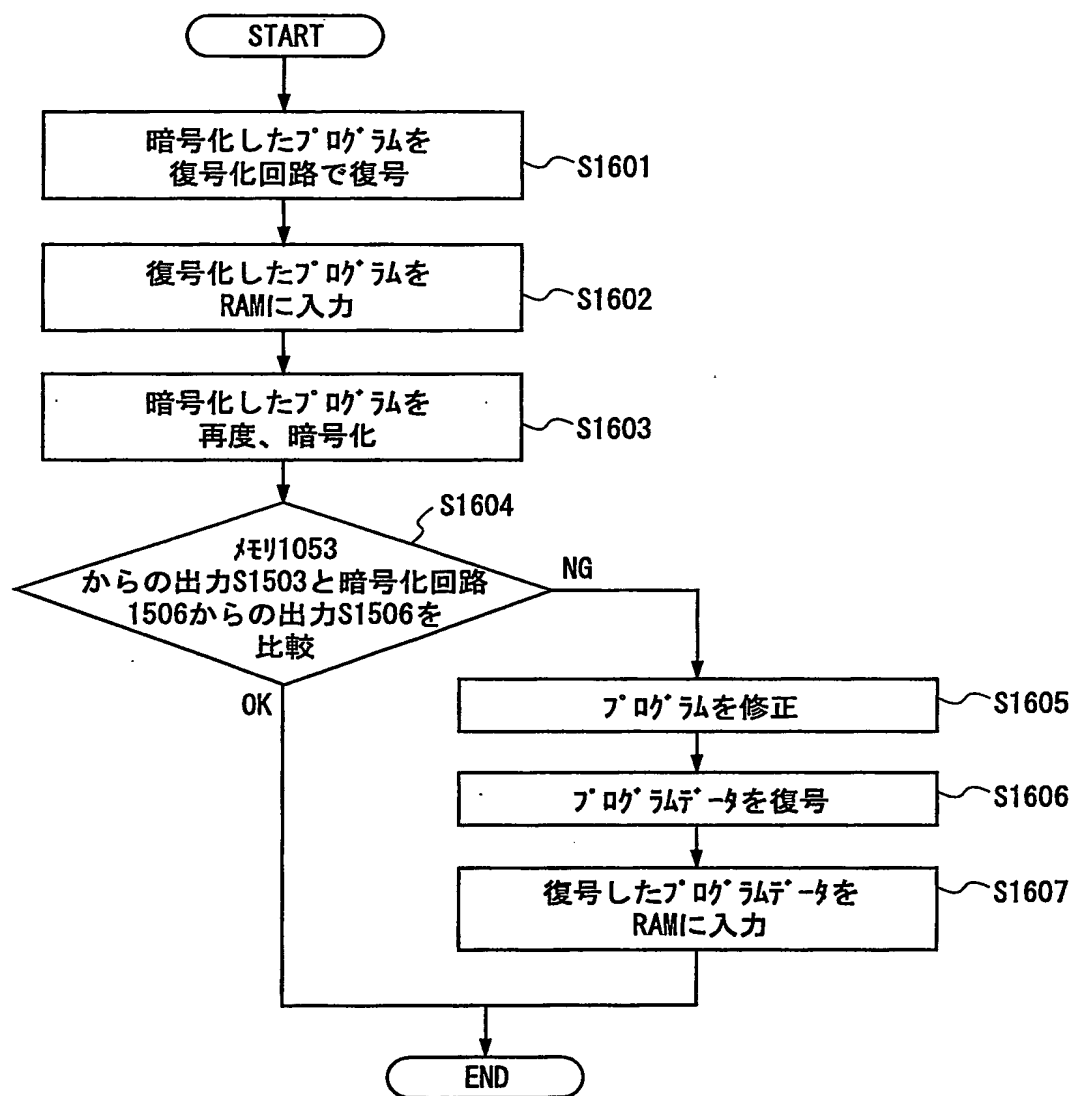
第14図



第15図

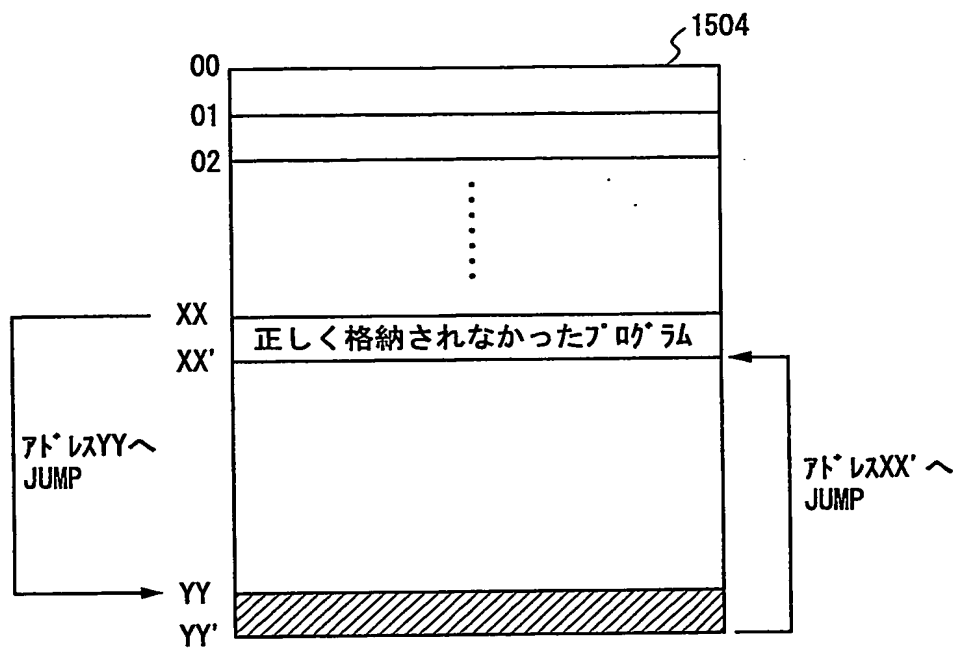


第16図



12/12

第17図



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/07541

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F12/14, G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F12/14, G06F1/00, G06F9/06, G06F12/16

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2003  
Kokai Jitsuyo Shinan Koho 1971-2003 Jitsuyo Shinan Toroku Koho 1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 5-66937 A (Oki Electric Industry Co., Ltd.), 19 March, 1993 (19.03.93), All pages; all drawings (Family: none)	2-14 15-19, 22-30, 33-40 1
X Y A	JP 2000-148502 A (NEC Corp.), 30 May, 2000 (30.05.00), All pages; all drawings (Family: none)	2-14 15-19, 22-30, 33-40 1
X Y A	JP 10-11279 A (Tamura Electric Works, Ltd.), 16 January, 1998 (16.01.98), All pages; all drawings (Family: none)	2-14 15-19, 22-30, 33-40 1

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:  
"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier document but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
04 September, 2003 (04.09.03)

Date of mailing of the international search report  
16 September, 2003 (16.09.03)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/07541

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 62-67800 A (Hitachi, Ltd.), 27 March, 1987 (27.03.87), All pages; all drawings & EP 215464 A2 & US 4777586 A & US 4905142 A	21, 32 19, 22-28, 30, 33-39
X Y	JP 63-186330 A (Anritsu Corp., Nippon Telegraph And Telephone Corp.), 01 August, 1988 (01.08.88), All pages; all drawings (Family: none)	21-23, 32-34 19, 24-28, 30, 35-39
X Y	JP 7-105169 A (NEC Corp.), 21 April, 1995 (21.04.95), All pages; all drawings (Family: none)	21, 32 19, 22-28, 30, 33-39 23, 34
X Y	JP 11-282756 A (Nakamichi Corp.), 15 October, 1999 (15.10.99), All pages; all drawings (Family: none)	19, 21, 22, 24-28, 30, 33, 35-39
Y	JP 63-240629 A (Nicksdorf Computer AG.), 06 October, 1988 (06.10.88), All pages all drawings & EP 280035 A2 & US 5224160 A	15-18, 28, 39
Y	JP 6-259242 A (Hitachi, Ltd.), 16 September, 1994 (16.09.94), All pages; all drawings; particularly, Par. No. [0009] (Family: none)	29, 40

# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/07541

## Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☒ Claims Nos.: 20, 31  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:  
Claims 20 and 31 do not describe necessary matters and what is described is unclear. The description "secret data stored in area which cannot be accessed from outside" contradicts the description "a specific part of the secret data is output outside".
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

## Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claim 1 relates to a technical feature used after a program stored in the second storage means is rewritten by the rewrite program stored in the first storage means and validity is checked, for storing the rewrite program in the external read out disabled area of the second storage means.

claims 2-6 relate to a technical feature for rewriting the program stored in the second storage means by the rewrite program stored in the first storage means and executing the rewritten program in the second storage means.

(continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.  
☐ No protest accompanied the payment of additional search fees.



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/07541

Continuation of Box No.II of continuation of first sheet(1)

Claims 7-14, 16, 17, 28, and 39 relate to a technical feature for judging validity of the program when the program stored in the second storage means is rewritten by the rewrite program stored in the first storage means.

Claims 15 and 18 are not so linked as to form a single general inventive concept.

Claims 19 and 30 relate to a technical feature for storing arbitrary data in an area accessible from outside and when stored correctly, secret data is stored in an area inaccessible from outside.

Claims 21-27 and 32-38 relate to a technical feature for outputting only the program execution result stored in the area inaccessible from outside.

Claims 29 and 40 relate to a technical feature for judging program validity for each instruction and when the result is invalid, jump is performed to a valid program newly stored.

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F12/14, G06F1/00

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl<sup>7</sup> G06F12/14, G06F1/00, G06F9/06, G06F12/16

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926 - 1996

日本国公開実用新案公報 1971 - 2003

日本国登録実用新案公報 1994 - 2003

日本国実用新案登録公報 1996 - 2003

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 5-66937 A (沖電気工業株式会社) 1993.03.19, 全頁, 全図 (ファミリーなし)	2-14
Y		15-19, 22-30, 33-40
A		1

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&amp;」 同一パテントファミリー文献

国際調査を完了した日

04.09.03

国際調査報告の発送日

16.09.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号 100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

奥村 元宏

5N

3044

電話番号 03-3581-1101 内線 3585

C (続き) 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2000-148502 A (日本電気株式会社) 2000.05.30, 全頁, 全図 (ファミリーなし)	2-14
Y		15-19, 22-30, 33-40
A		1
X	JP 10-11279 A (株式会社田村電機製作所) 1998.01.16, 全頁, 全図 (ファミリーなし)	2-14
Y		15-19, 22-30, 33-40
A		1
X	JP 62-67800 A (株式会社日立製作所) 1987.03.27, 全頁, 全図 & EP 215464 A2 & US 4777586 A & US 4905142 A	21, 32
Y		19, 22-28, 30, 33-39
X	JP 63-186330 A (アンリツ株式会社、日本電信電話株式会社) 1988.08.01, 全頁, 全図 (ファミリーなし)	21-23, 32-34
Y		19, 24-28, 30, 35-39
X	JP 7-105169 A (日本電気株式会社) 1995.04.21, 全頁, 全図 (ファミリーなし)	21, 32
Y		19, 22-28, 30, 33-39
X	JP 11-282756 A (ナカミチ株式会社) 1999.10.15, 全頁, 全図 (ファミリーなし)	23, 34
Y		19, 21, 22, 24-28, 30, 33, 35-39
Y	JP 63-240629 A (ニクスドルフ・コンピュータ・アクチエンゲゼルシャフト) 1988.10.06, 全頁, 全図 & EP 280035 A2 & US 5224160 A	15-18, 28, 39
Y	JP 6-259242 A (株式会社日立製作所) 1994.09.16, 全頁, 全図, 特に【0009】段落 (ファミリーなし)	29, 40

## 第Ⅱ欄の続き

請求の範囲 1 5 及び 1 8 は、単一の一般的発明概念を形成しているとはいえない。

請求の範囲 1 9 及び 3 0 は、任意のデータを外部からアクセス可能な領域に記憶し、正しく記憶された場合、外部からアクセス不可能な領域に機密データを記憶する技術に関するものである。

請求の範囲 2 1 - 2 7 及び 3 2 - 3 8 は、外部からアクセス不可能な領域に記憶されているプログラムの実行結果のみを外部に出力する技術に関するものである。

請求の範囲 2 9 及び 4 0 は、プログラムの正当性を命令毎に判断し、正当でないと判定された場合には新たに記憶した正当なプログラムのアドレスへジャンプする技術に関するものである。

## 第 I 欄 請求の範囲の一部の調査ができないときの意見 (第 1 ページの 2 の続き)

法第 8 条第 3 項 (P C T 1 7 条 (2) (a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 \_\_\_\_\_ は、この国際調査機関が調査をすることを要しない対象に係るものである。  
つまり、
2. ☒ 請求の範囲 20, 31 は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、  
請求の範囲 2 0 及び 3 1 には、必要な事項が記載されておらず、また、その記載も著しく不明瞭である。「外部からアクセス不可能な領域に記憶された機密データ」及び「機密データの特定部分を外部に出力する」という記載は矛盾する。
3. ☐ 請求の範囲 \_\_\_\_\_ は、従属請求の範囲であって P C T 規則 6. 4 (a) の第 2 文及び第 3 文の規定に従って記載されていない。

## 第 II 欄 発明の単一性が欠如しているときの意見 (第 1 ページの 3 の続き)

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

請求の範囲 1 は、第 2 の格納手段に格納されたプログラムを第 1 の格納手段に格納された書き換えプログラムにより書き換える際に、正当性の判定の後、書き換えプログラムを第 2 の格納手段の外部読出し不可能領域に格納する技術に関するものである。  
請求の範囲 2 - 6 は、第 2 の格納手段に格納されたプログラムを第 1 の格納手段に格納された書き換えプログラムにより書き換えた後に、第 2 の格納手段の書き換えられたプログラムを実行する技術に関するものである。  
請求の範囲 7 - 1 4, 1 6, 1 7, 2 8 及び 3 9 は、第 2 の格納手段に格納されたプログラムを第 1 の格納手段に格納された書き換えプログラムにより書き換える際に、プログラムの正当性の判定を行う技術に関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。  
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。